DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/LAS/97D-10

AN ANALYSIS OF UNCLASSIFIED CURRENT AND PENDING AIR FORCE INFORMATION WARFARE AND INFORMATION OPERATIONS DOCTRINE AND POLICY

THESIS

Kenneth V. Peifer, Captain, USAF

AFIT/GIR/LAS/97D-10

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

AFIT/GIR/LAS/97D-10

AN ANALYSIS OF UNCLASSIFIED CURRENT AND PENDING AIR FORCE INFORMATION WARFARE AND INFORMATION OPERATIONS DOCTRINE AND POLICY

THESIS

Presented to the Faculty of the Graduate School of Logistics

and Acquisition Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Information Resource Management

Kenneth V. Peifer, B.S.

Captain, USAF

December 1997

Acknowledgments

This thesis could not have been completed without the support and encouragement of many people. I thank my advisor, Dr. Alan Heminger for his insight and open-mindedness toward the phenomenon known as Information Warfare, his great patience, and especially for helping me as a mentor in Information Resource Management.

I owe a great debt of gratitude to Major Bill Scott who enlightened me in the importance of sound methodology.

My sponsor, Mrs. Dora Ojeda of the Air Force Information Warfare Center's Engineering Analysis directorate put me in contact with many knowledgeable people working in the Information Warfare arena. These contacts were of critical importance to the completion of this thesis.

I also wish to thank Dr. Norman Ware, who provided thoughtful criticism and an undeserved measure of patience and kindness to me as my Reader.

I especially wish to thank my wife Leila, and my daughter Ingrid. Without their love and understanding, I would not have completed this work.

Kenneth V. Peifer

Table of Contents

List of Figures

List of Tables

Abstract

Previous studies concerning information warfare doctrine and policy attempted to define and describe concepts, issues and develop ideas. From these studies and other sources, high level guidance has been mandated, published, and to a certain extent implemented. A logical next step is to study what has been done at the military service level to engage information warfare and the larger information operations.

This study focused on determining if unclassified current and pending Air Force information warfare and information operations doctrine and policy is moving in the direction it should in terms of being complete, consistent and cohesive based on what has been mandated and studied about these two phenomena.

Investigative questions were developed in reference to the current state of unclassified Air Force information warfare and information operations doctrine and policy. Secondary data analysis was conducted along two paths. The hierarchical path included an examination of unclassified information warfare and information operations doctrine, policy and regulatory guidance. The academic path included an examination of studies and commentary on information warfare and information operations focusing on doctrine and policy. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was developed. Then the model was analyzed for congruence in terms of completeness, consistency, and cohesiveness using the hierarchical and academic secondary data analysis as a diagnostic tool. The model was found to be partially incongruent in all three areas.

AN ANALYSIS OF UNCLASSIFIED CURRENT AND PENDING AIR FORCE INFORMATION WARFARE AND INFORMATION OPERATIONS DOCTRINE AND POLICY

I. Introduction

Know the enemy and know yourself; in a hundred battles you will never be in peril.
- Sun Tzu (Tzu, 84)

The Vague Notion of Information Warfare

The basic concept of information warfare (IW) is not new; it has been a part of war-making science since ancient times. Long before the advent of high-speed digital circuitry, warring factions attempted to protect and employ their information in the conduct of war while attacking and otherwise exploiting the enemy's information.

Advances in technology have changed the essence and means of IW, and in the process drastically altered its nature if not its goal. Conceptualizing the raw scope of IW has become a daunting task in itself, perplexing some, confusing many and making it difficult to not only know who the enemy is, but to recognize oneself as well.

To begin with, there are many, perhaps too many, definitions of IW in cyberspace as well as in print. There are several used within the Department of Defense (DOD) alone, which makes it difficult to begin to understand the military perspective of IW. Two are listed below to illustrate this point.

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [CJCSI 3210.01, 1996] (SAIC, B-73)

> Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. (Cornerstones, 13), (AFDD 50, 10)

In a 1995 essay entitled "What Is Information Warfare?", Martin Libicki attempted to sort out several possible definitions of IW by identifying seven competing forms (Libicki, Preface):

1. Command-and-Control Warfare
2. Intelligence-Based Warfare
3. Electronic Warfare
4. Psychological Warfare
5. Hacker Warfare
6. Economic Information Warfare
7. Cyberwarfare

Winn Schwartau, an author and lecturer on IW divides it into three environmentally "distinct levels of intensity" or classes (Schwartau, 32-36):

1. Class 1: Personal Information Warfare
2. Class 2: Corporate Information Warfare
3. Class 3: Global Information Warfare

Although these forms and classes may help develop a framework for identifying what IW is, none has the distinct advantage of capturing its definition entirely.

Another difficulty with understanding what IW is, from a military perspective, beyond trying to define it, is that it has multiple aspects or dimensions, such as offensive and defensive, technological, legal, policy and doctrinal, infrastructural and organizational. Each of these is nomologically related, and therefore, they must be considered together in a unified construct to fully understand what IW entails.

Currently, there is a movement within the DOD away from identifying this phenomenon as Information Warfare in favor of Information Operations (IO). Examples of this movement are discussed in Chapter II in the review of Joint Publication 3-13, *Joint Doctrine for Information Operations*, Air Force Doctrine Document 1, *Air Force Basic Doctrine*, and Air Force Doctrine Document 2-5, *Information Operations*. IW may be viewed as a subset of IO: conducted under hostile circumstances. It is unknown whether this new term will be universally adopted.

Each of the services has taken a different direction in pursuit of operationalizing IW. The Army has implemented Force XXI, which integrates IW activity across all (Army) Major Commands (MAJCOMs) and includes Land Information Warfare Activity (LIWA), and Field Manual 100-6 *Information Operations*, a doctrine for Army IW, the first of its kind among the services (SAIC, A-33). The Navy has several organizational divisions responsible for IW operations, planning, policy and strategy. The Naval Information Warfare Activity (NIWA) is the principal technical agent in pursuing IW technologies. The Fleet Information Warfare Center (FIWC) was established in October 1995 as the Navy's IW Center of Excellence. FIWC is responsible for IW operations, tactics, procedures and training (SAIC, A-38). The Air Force has refined the definition of IW. The result is Information Operations (IO), which are "actions taken to affect adversary information and information systems while defending one's own information, and information systems" (AFIWC briefing, 7 Aug 97). Information Warfare is then "IO conducted primarily during time of crisis or conflict to achieve information superiority

and other military objectives" (AFIWC briefing, 7 Aug 97). The Deputy Chief of Staff for Operations (XO) serves as the lead for coordinating IW doctrine within the Air Force. The Air Force has taken an integrated approach to IW. The result is that many line and staff organizations are involved, at various levels, in developing and integrating doctrine, policy, plans, programs and procedures across the service (SAIC, A-54). The Air Force Information Warfare Center (AFIWC) was established in October 1993. The AFIWC is somewhat similar to the Navy's FIWC: supporting operations, planning and testing by developing, maintaining and deploying Information Warfare/Command and Control Warfare (IW/C2W) capabilities (AFIWC Mission and Goals, 1). With fewer resources, the Marine Corps works with the other services in pursuit of IW capabilities. There are Marine billets in the NIWA, FIWC, and AFIWC to support Marine IW operations (SAIC, A-49).

Another point of confusion and some argument is, What exactly are the boundaries of military IW and IO? To answer this question, we must first know what the military IW and IO responsibilities are. The good news is that there is a lot of insightful and comprehensive work underway to clear the smoke of the IW and IO constructs. Forums, conferences, research and education are bringing about more than simple awareness. We are gaining ground towards a deep understanding of the IW and IO complexities and are humbly realizing we are not as IW/IO-smart as we thought we were. Hopefully IW and IO are becoming less vague as we prepare to cross the threshold into the 21st century.

The Mounting Threats To Our National Information Infrastructure

The threats to national security and the nation's information infrastructures posed by IW and IO are large. But before examining examples of the threats, it will be useful to establish a framework of Information Infrastructures (IIs). IIs consist of the information, modes of storage and conveyance, the physical equipment, and the people who use the information within a domain. It is critical to understand that the formation of IIs was a direct result of advances in information technologies, primarily those that enable connectivity. A suggested model, depicted in Figure 1, recognizes a few of the key IIs that exist within the overarching Global Information Infrastructure (GII).

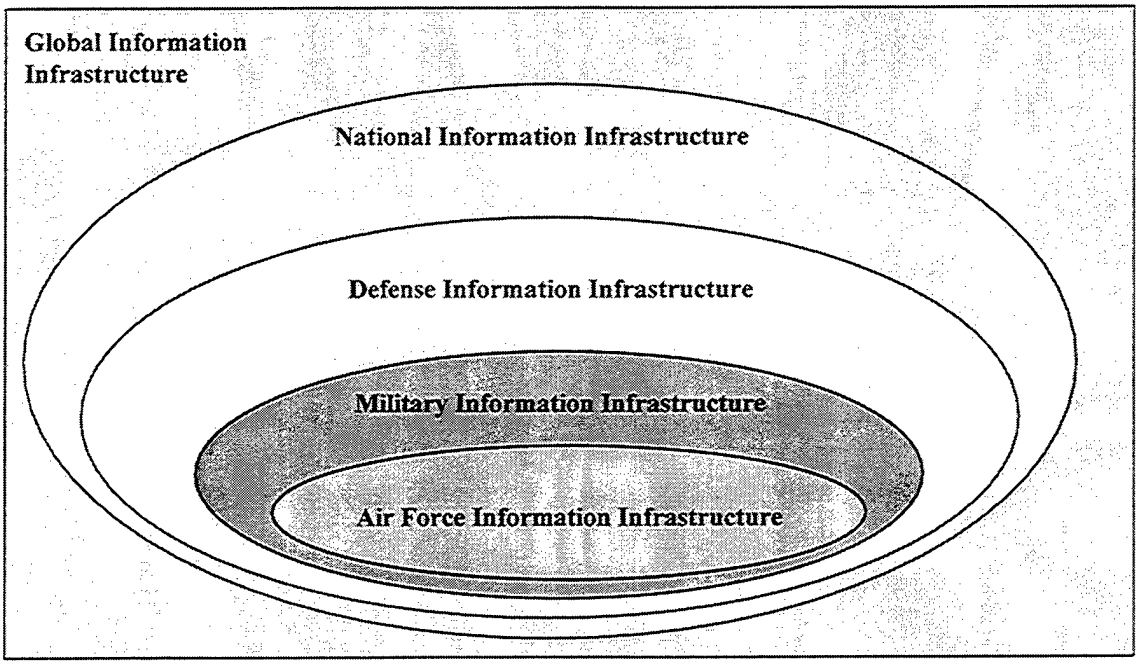


Figure 1. Key Information Infrastructures Model

The National Information Infrastructure (NII) is couched in the GII. It contains commercial, industrial, academic, governmental, and telecommunications domains (JCS brochure, 2). The Defense Information Infrastructure (DII) resides within the NII as part of the government domain. Within the DII is the Military Information Infrastructure (MII). The MII is comprised of the service domains; Army, Navy, Air Force and Marine Corps. The Air Force Information Infrastructure (AFII) consists of the Air Force's segment of the MII. Each of the infrastructures depicted in the model is either directly or indirectly connected to the others, as well as to other infrastructures and domains not depicted.

The model as shown in Figure 1 is certainly not all-inclusive. The MII for instance is composed of the individual service information infrastructures which have been intentionally left out. The Geospatial Information Infrastructure permeates the entire model but is also not explicitly depicted in Figure 1. Also, there are non-military information infrastructures within the DII that are not depicted in the model such as those of the National security Agency (NSA), National Institute of Standards and Technology (NIST), Central Intelligence Agency (CIA) and National Reconnaissance Office (NRO) domains. For purposes of this examination, the model has been kept as simple as possible. The object is to identify the hierarchy and relationships of several key information infrastructures.

In 1996 WarRoom Research, LLC conducted an Information Systems Security Survey which had been developed in coordination with the U.S. Senate Permanent Subcommittee on Investigations. The Subcommittee had been investigating threats and

vulnerabilities of our nation's NII. The survey targeted Fortune 1000 firms that are part of our nation's NII, as well as the GII. Results of the survey indicated that 98 of the 205 firms responding had experienced intrusions by outsiders to their computer systems. The cost per incident of these intrusions was estimated to be over $50,000 by 84 percent of those who responded. Also, 31 firms reported estimated losses over $500,000, and 36 firms reported losses over $1,000,000 (WarRoom Research news release).

A May 1996 report on Pentagon computer security (GAO/AIMD-96-84) serves as a prime example of the current state of affairs within the DII. The report identified the extent of attacks on defense computer systems as both a "multimillion dollar nuisance to Defense" and "a serious and growing threat" (GAO, 3). The report stated;

> The potential for catastrophic damage is great. Organized foreign nationals or terrorists could use information warfare techniques to disrupt military operations by harming command and control systems, the public switch network, and other systems or networks Defense relies on. (GAO, 3)

In November 1996, the Defense Science Board (DSB) Task Force on Information Warfare Defense was released. The report summarized validated threats to our NII that were obtained from a variety of NII sources. The report marked several incidents over the past decade that are characterized as IW threats. They include:

1. The Hanover Hackers who penetrated a myriad of computer systems to eventually reach several military installations worldwide (late 1980s),
2. Software time bombs in Public Network switches in Denver, Atlanta, and New Jersey (mid-1989),
3. Dutch teenagers intrusion into Pentagon computers during the Gulf War (Nov 1991),

4. Rome Labs intrusion via the Internet (Apr 1994), and,

5. An account of an Air Force Captain hacking into U.S. Atlantic Fleet ship computers as a system vulnerability test (Sept 1995) (DSB, Appendix A, 5) and (Stoll, diagram).

The AFIWC gathers statistics on a variety of IW incidents and threats involving Air Force computer systems. In the last year there was a rise in the number of virus attacks; from 583 reported incidents in 1995, to 896 in 1996. The damage in lost hours alone is immense; 2,719 (1995) and 7,950 (1996). Incident/Intrusion Statistics showed a slight decrease in the number of intrusions into Air Force systems; 25 in 1995 and 20 in 1996 (AFIWC summary, 1).

The intrusions and attacks described above involve both commercial and government computer systems. They are demonstrative of the threat that exists to our NII's industrial, commercial and economic domains as well as the threat to the DII and MII. These infrastructures and systems play a vital role in our national security. If entire power grids go down, if data files containing corporate secrets are stolen, or if electronic commerce systems become corrupted, our nation's security, productivity and citizens will suffer. Threats to these infrastructures and systems are threats to our livelihood and our way of life.

The Need for Air Force IW and IO Policy and Doctrine

It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's own self invincible.

- Sun Tzu (Tzu, 114)

We must assume the IW enemy is coming. The previous section (The Mounting Threats to Our National Information Infrastructure), demonstrates that the enemy is here and capable. We need doctrine and policy that will allow us to meet the enemy in battle and to make us invincible.

In *Cornerstones of Information Warfare*, the Secretary of the Air Force, and Air Force Chief of Staff offered a description of how Air Force doctrine should evolve to encompass information warfare. Drawing from existing doctrine, which recognizes air and space warfare, they described information warfare as cutting across all roles and missions and having the same objectives as air warfare. The resulting information warfare objectives are to:

1. control the information realm so it can be exploited while protecting (U.S.) military information functions from enemy action,

2. exploit control of information to employ information warfare against the enemy, and,

3. enhance overall force effectiveness by fully developing military information functions (Cornerstones of Information Warfare, 7-8).

Cornerstones of Information Warfare provides the Air Force with a starting point, but stops short of providing "a standard against which to measure our efforts" as doctrine should according to the introduction of volume 1 of Air Force Manual 1-1 (AFM 1-1, v1,

1992). Draft 4 of Air Force Doctrine Document (AFDD) 2-5, *Information Operations* contains the core of Air Force IO and IW doctrine. These documents form the nucleus of Air Force IO doctrine and policy. Together they are an authoritative confirmation that IW doctrine and policy are required at the Air Force level.

The Need for Integration

The previously discussed GAO report on Pentagon computer security (GAO/AIMD-96-84), stated that although attempts to react to successful computer attacks were underway, there was no uniform policy in place for assessing risks and damage, or for system protection. The report stated that user, system and network administrator training were inconsistent and constrained by limited resources. The report also indicated that the success of measures to protect Defense information and systems depended on having better policy (GAO, 3).

The November 1996 Defense Science Board (DSB) Task Force on Information Warfare Defense report focuses on protection of (national) information interests through the development of an information warfare defense capability. The report lists over 50 recommendations to prepare the DOD for information warfare with a 5 year $3 billion budget (DSB, 10).

The top recommendation was to designate the Assistant Secretary of Defense (ASD) for C3I as the accountable focal point for all information warfare issues. Among other responsibilities, the ASD for C3I would be charged with promulgating an integrated information warfare policy (DSB, 10).

It is clear that the intent of the DSB's recommendations is that IW policy be completely integrated. This appears to make sense since our information infrastructures are inter-networked and integrated in many ways.

In a Joint Chiefs of Staff brochure which outlines basic and integrated IW concepts, General Shalikashvili, discusses the need an for integrated IW posture. He states "Information Warfare (IW) has emerged as a key joint warfighting mission area" (JCS brochure, From the Chairman). He goes on to state the importance of fully developed and integrated IW capabilities in support of warfighters, (JCS brochure, From the Chairman) and that IW applies across all phases, the range of military operations, and at every level of warfare (JCS brochure, 4). The brochure points out that the Joint Staff will lead the development efforts for (joint) IW doctrine to ensure that there is a common vision in all IW efforts (JCS brochure, 17-20).

Neither the Air Force, nor any other service, agency, nor governmental department can continue to forge ahead in a vacuum. Integrated IO/IW doctrine, policies, and offensive and defensive operations are being called for from the highest offices in government. Recognition of the GII, NII, DII, MII and other related domains will be key to complete integration.

The Need for Doctrine and Policy Analysis

The preceding sections of this introduction intended to establish a basis for why Air Force IO and IW doctrine and policy should be analyzed. First, IW continues to be a vague notion, lacking a universal definition for the military, approached differently by

each service, and, a phenomenon we as a nation have not yet mastered. The larger "information operations" construct is also not fully understood.

The mounting threats to our NII posed by IW also threaten the Air Force. The Air Force is a stakeholder in the MII, the NII and GII as well as its own AFII, and continues to be attacked daily.

Does Air Force IO and IW doctrine and policy flow naturally and consistently from guidance developed at higher levels? Does the Air Force understand its place in Information Infrastructures policy formulation? It is clear that there is a need for Air Force IO and IW doctrine and policy. Does it address everyone it needs to at all appropriate levels?

Finally, there is strong authoritative guidance that all IO and IW doctrine and policy should be integrated seamlessly to support our national strategic objectives and our national security. Is the Air Force IO and IW doctrine and policy consistent with our national strategic objectives and national security?

An analysis of current and pending unclassified Air Force IO and IW doctrine and policy can address these questions and hopefully provide information and suggestions to ensure that the objectives of information superiority are met.

Drawing from what has been mandated, studied and suggested regarding military response to IO and IW, this thesis analyzes current and pending unclassified Air Force IO and IW doctrine and policy. The specific investigative research questions answered are:

1. Does Air Force IO and IW doctrine and policy flow naturally and consistently from guidance developed at higher levels?

2. Is Air Force IO and IW doctrine and policy complete?

3. Does Air Force IO and IW doctrine and policy address everyone it needs to at all appropriate levels?

4. Is Air Force IO and IW doctrine and policy consistent with our national strategic objectives and national security?

An Overview of the Research

Chapter II discusses how IO and IW doctrine and policy are formed at the Air Force and Joint-levels through a presentation of the Air Force and Joint doctrine processes, provides a chronology of documentation central to IO and IW doctrine and policy formation, and presents a compendium of documentation that addresses key issues in IO and IW doctrine and policy development from hierarchical and academic perspectives. Chapter II also provides a summary of the key IO and IW policy and doctrine issues. Chapter III discusses the research methodology. It describes the nature of an exploratory study, criterion-based congruence analysis, application of the Delphi technique, and research assumptions. Chapter IV presents the results of the Delphi group and the results of the criterion-based congruence analysis. Chapter V discusses how the results of the congruence analysis apply to the specific investigative questions, provides observations regarding Air Force IO and IW doctrine and policy, and identifies the limitations of the study. It also suggests further research avenues.

II. Literature Review

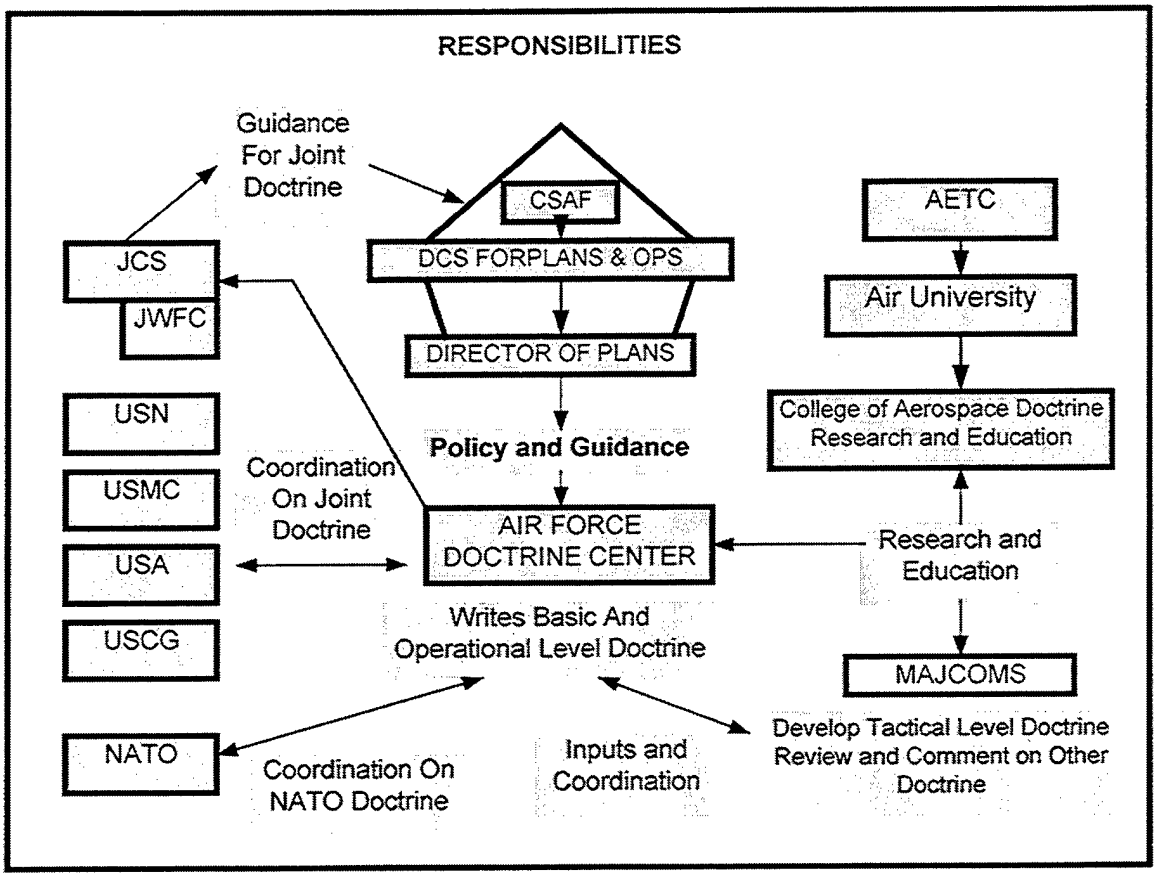
This chapter provides an overview of IO and IW doctrine and policy processes at the Air Force and Joint Chiefs of Staff levels. A chronology of documentation central to IO and IW doctrine and policy development is also presented, along with relevant research and commentary that touch on key issues in IO and IW doctrine and policy formation. The chapter concludes with a summary of the key IO and IW doctrine and policy issues.

The Formation of Air Force IO and IW Doctrine and Policy

The formation of Air Force IO and IW doctrine and policy is by and large the result of an evolutionary set of processes happening concurrently at multiple levels throughout the DOD and beyond. The processes can be grouped into two major processes of doctrine and policy development: the Air Force process, and the Joint process. Each of these major processes is presented in the following paragraphs.

The Air Force Process. The Air Force has established an organizational structure, which is part of a larger multi-agency structure, for developing doctrine. The Chief of Staff of the Air Force has overall responsibility for Air Force doctrine. At the heart of the process is the Air Force Doctrine Center (AFDC), which is responsible for writing basic and operational level doctrine, including Information Warfare doctrine. Figure 2 depicts the current process for the development of doctrine in the Air Force. It is clear from this figure that many organizations outside the AFDC are involved in the process, and that

they contribute by providing input to, and coordination on the overall doctrine and policy development effort (DAF, Linhard, slide 8, 1996).



(Adapted from DAF, Linhard, slide 8, 1996)

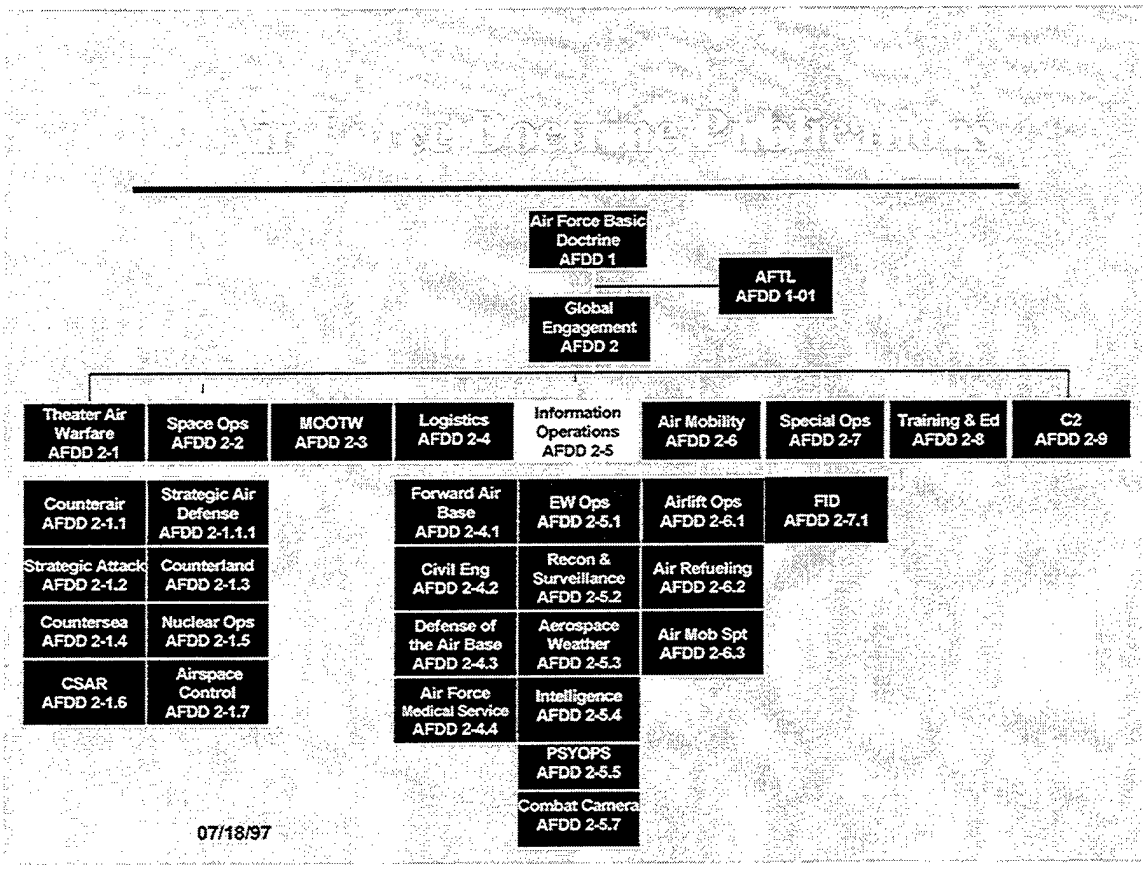
Figure 2. Doctrine Development Process for the Air Force

As an evolutionary process, doctrine and policy development is dynamic and subject to constant change and revision. An example of this evolution can be found in the drafting of information operations doctrine.

As of this writing, AFDD 2-5 *Information Operations*, is in draft coordination. This document is at the center of Air Force information operations doctrine. During a series of revisions beginning in 1995 this document changed in content to reflect new thinking in IO/IW concepts. This also led to a change in title. The title changed from AFDD 5 *Information Warfare*, as it was in November of 1995 in the first draft, to AFDD 5 *Information Operations*, when it was presented as draft 2 in October of 1996. Draft 3, dated 9 May 1997, was entitled AFDD 2-5, *Information Operations*. This latest title change reflects a realignment of the doctrine numbering scheme, bringing it under AFDD 2, *Global Engagement* (see Figure 3. Current and Pending Air Force Doctrine Documents). The title of AFDD 2 is currently *Air and Space Power Organization and Employment*, and it is in its 7th draft version. These changes may appear minor or insignificant, but they aptly demonstrate the dynamic nature of doctrine development.

The title change from *Information Warfare*, to *Information Operations* is significant, reflecting a confirmation of a paradigm shift occurring in IW theory. Current thought recognizes IW as the state of Information Operations (IO) conducted during a crisis to achieve information superiority (AFDD 2-5, 9 May 97, 3rd draft).

Figure 3 graphically depicts a snapshot of what the Air Force doctrine development process yields as of 19 July 1997.

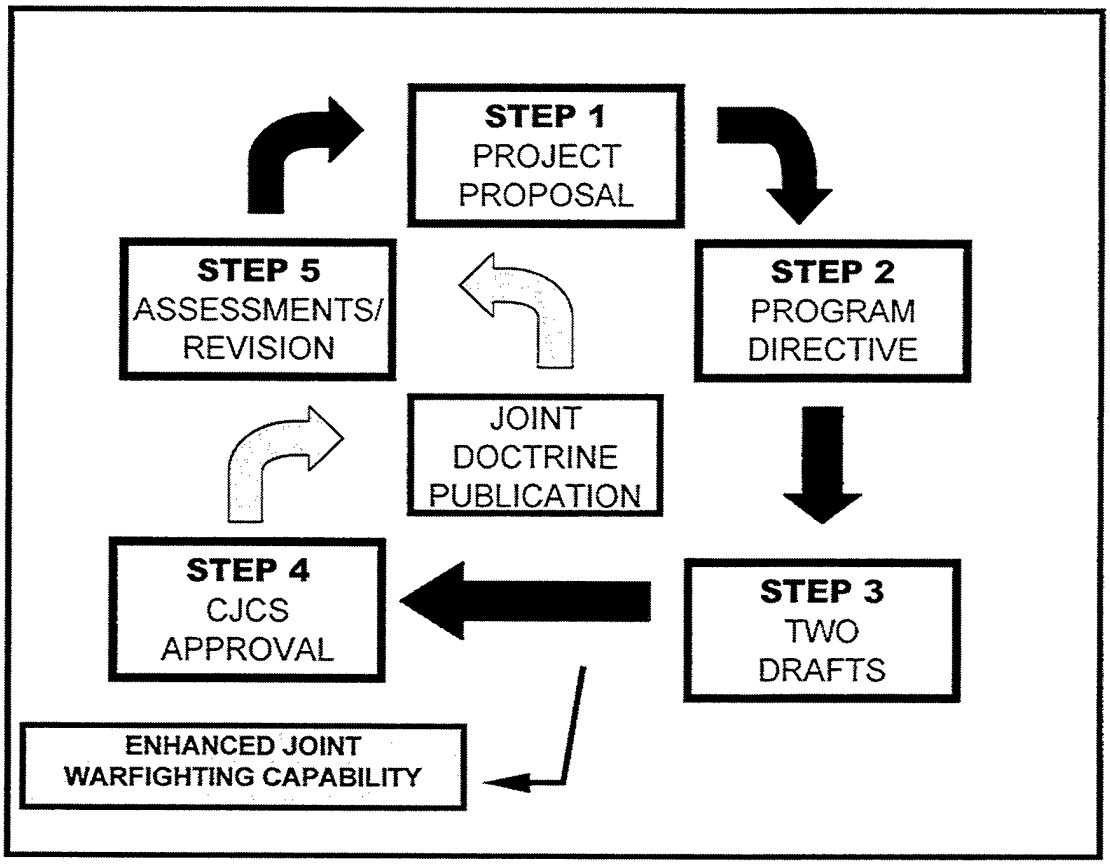


(Adapted from AFDC/XDD briefing slide)

Figure 3. Current and Pending Air Force Doctrine Documents

The JCS Process. The Joint doctrine process obtains inputs from the Services, the Joint Staff, and the combatant commands. The process follows five distinct steps. The steps include Project Proposal, Program Directive, Two Drafts, CJCS Approval, and Assessments/Revision.

Figure 4. Joint Doctrine ProcessFigure 4, depicts this process. The details of each step are presented below Figure 4 and on the following page.



(Adapted from JCS Doctrine Process Chart, 10 October 1997)

Figure 4. Joint Doctrine Process

STEP #1 Project Proposal
- Submitted by Services, CINCS, or Joint Staff to fill operational void
- validates requirement with Services and CINCs
- initiates Program Directives

STEP #2 Program Directive
- staffs with Services and CINCs
- Includes scope of project, references, milestones, and who will develop drafts
- releases Program Directive to Lead Agent. Lead Agent can be Service,
- CINC, or Joint Staff (JS) Directorate

STEP #3 Two Drafts
- Lead Agent selects Primary Review Authority (PRA) to develop the pub
- PRA develops two draft pubs
- PRA staffs each draft with CINCs, Services, and Joint Staff

STEP #4 CJCS Approval

- Lead Agent forwards proposed pub to Joint Staff
- Joint Staff takes responsibility for pub, makes required changes and prepares pub for coordination with Services and CINCs
- Joint Staff conducts staffing for approval as a Joint Publication

STEP #5 Assessments/Revision

- The CINCs receive the pub and begin to assess it during use
- to 24 months following publication, the Director, J-7 solicits a written report from the combatant commands and Services on the utility and quality of each pub and the need for any urgent changes or earlier-than-scheduled revisions
- No later than 5 years after development, each pub is revised

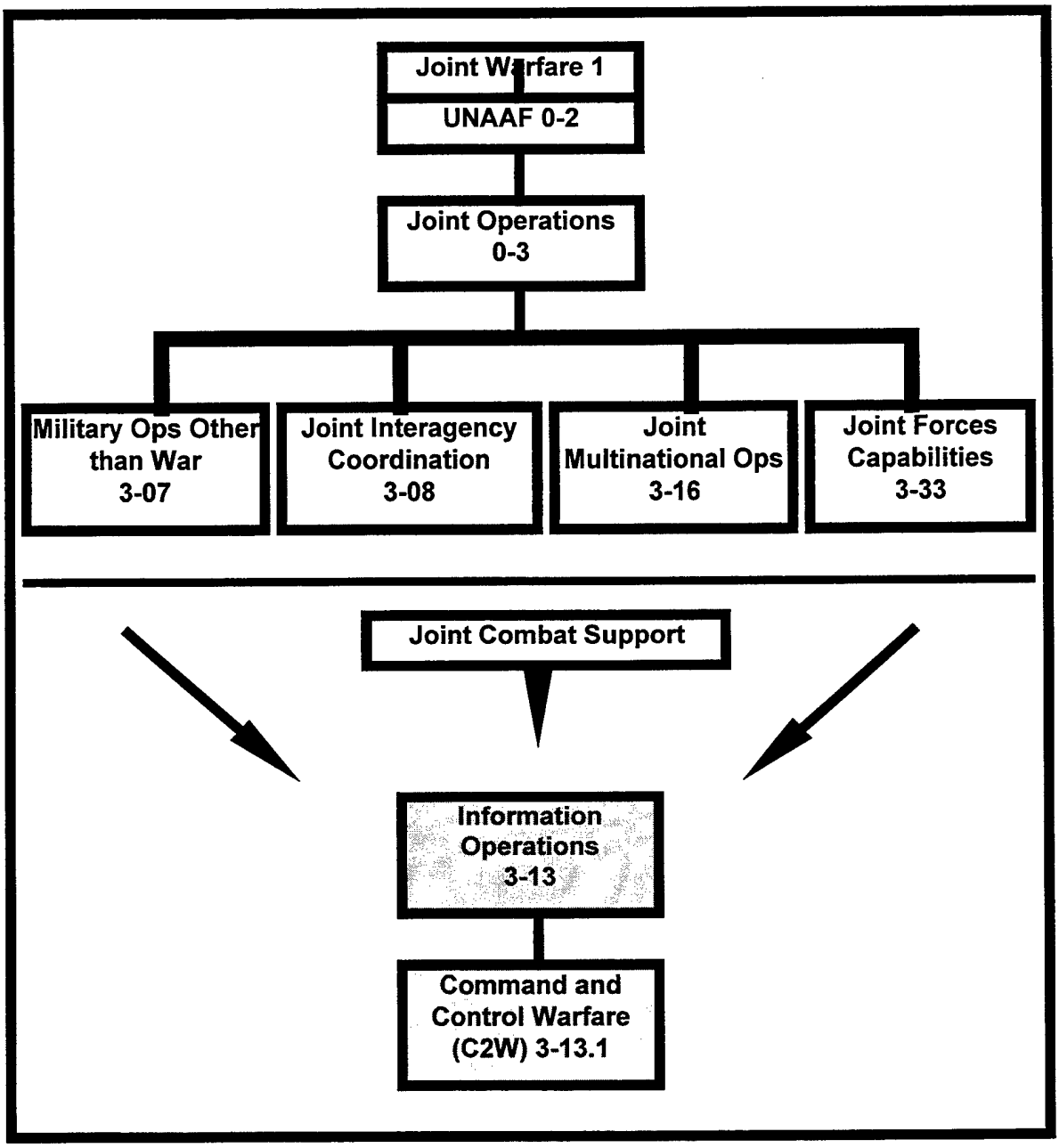
(JCS, Joint Doctrine Process, 10 October 1997)

Like the Air Force doctrine development process, Joint doctrine development is evolutionary and in a constant state of flux. The overarching document for all Joint publications is Joint Publication (JP) 1, *Joint Warfare of the Armed Forces of the United States*. The current version of this publication is dated 10 January 1995.

The entire Joint doctrine hierarchy consists of over one hundred publications; thirty percent of these are currently under development.

JP 3-13, *Joint Doctrine for Information Warfare* is still under development. Its first draft was dated 21 January 1997. An update to the first draft was entitled *Joint Doctrine for Information Operations*, reflecting the same shift in IW theory as in the Air Force's AFDD 2-5, *Information Operations.*

The second draft of JP 3-13 was reviewed for this thesis. JP 3-13 is part of the 3-series, Joint Operations doctrine publications. It falls under the category of Joint Combat Support. Figure 5. Joint Publication Hierarchy - IOFigure 5 on the following page depicts where IO doctrine fits into the hierarchy of joint publications and doctrine.



(Adapted from Newhier.ppt, Joint Publication Hierarchy,
http://www.dtic.mil/doctrine/docinfo/pstatus/hierchart.htm, 10 October 1997)

Figure 5. Joint Publication Hierarchy - IO

A Chronology of IO and IW Doctrine and Policy Guidance

It is instructive to discuss the chronology of key documents that contribute to Air Force IO and IW doctrine and policy. However, this can quickly become a difficult task and the subject of intense debate. When did information warfare begin? Quite possibly, information warfare began thousands of years ago. This could lead the researcher to begin analyzing the Bible, or cave hieroglyphics, in an attempt to pinpoint exactly when information warfare was conscientiously being practiced. In sharp contrast, some refer to Desert Storm as the first information war. How does one arrive at a logical starting point for such a chronology? It is arguable as to what the best answer is.

Information warfare touches upon many aspects of national security. It is a topic whose breadth and depth into military and national affairs is still being realized. Advances in information technology, and particularly the advent of global connectivity, have drastically changed the notion of information warfare, and the refined construct referred to as information operations.

Assuming there is an identifiable starting point, a follow-up question is; how far into the wide span of IO and IW literature and doctrinal and policy guidance does one go to capture what is relevant for analysis?

Presented in Table 1 is a suggested chronology of IO and IW doctrine and policy guidance. It was derived by first examining pending IO-related doctrine and policy, and tracing its linkages backward through current doctrine and policy, reference material, and

associated research documents. Its purpose in this research is to provide answers to the questions of where to begin, and how far to go.

The objective of this approach was to establish a logical starting point to begin the research, and to set reasonable boundaries to properly scope the congruence analysis.

The resulting starting point for this research is the third draft of Air Force Doctrine Document (AFDD) 2-5, Information Operations, dated 9 May 1997. From this document, linkages were traced backward along two main categories of literature; Hierarchical, and Academic. The Hierarchical category includes specific IO and IW guidance, and general doctrine and policy guidance, formed laterally and from above the Air Force level at several tiers. The Academic category includes recent research and studies into IO and IW issues as they relate to strategy, doctrine, and policy formation.

Table 1 provides a number for each document, a short title (if applicable), long title, and a Category/Remarks section which indicates whether the document is categorized as Hierarchical or Academic. Listed in Table 1are only unclassified documents. Classified documents pertaining to IO and IW strategy, doctrine and policy were not reviewed, as this entire research effort is intended to remain unclassified.

Table 1. A Suggested Chronology of Key IO/IW Doctrine and Policy Guidance

#	Date	Short Title	Long Title	Category/Remarks
1	Mar 92	AFM 1-1	Basic Aerospace Doctrine of the United States Air Force	Hierarchical: general doctrinal guidance
2	12 Aug 93	AFPD 10-7	Air Force Policy Directive 10-7, *Operations*, Command and Control Warfare	Hierarchical: specific IW related guidance
3	95	n/a	Information Warfare, Airpower	Academic: specific

			Journal, George J. Stein	IW strategy and doctrine commentary
4	95	JV 2010	Joint Vision 2010, America's Military Preparing for Tomorrow (JCS)	Hierarchical: National Security guidance
5	95	n/a	New World Vistas, Air and Space Power for the 21st Century, Information Applications Volume	Academic: specific IW related guidance
6	95	n/a	New World Vistas, Air and Space Power for the 21st Century, Information Technology Volume	Academic: specific IW related guidance
7	95	n/a	National Military Strategy of the United States (JCS)	Hierarchical: National Security guidance
8	95	n/a	USAF Fact Sheet 95-20, Information Warfare	Hierarchical: specific IW information
9	10 Jan 95	JP 1	Joint Publication 1, Joint Warfare of the Armed Forces of the United States	Hierarchical: general joint doctrine guidance
10	1 May 95	ACSC/DEC/020/95-05	Information Warfare: An Opportunity for Modern Warfare	Academic: specific IW research USAF/ACSC
11	30 May 95	JP 6	Joint Publication 6, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations	Hierarchical: joint IW related guidance
12	Jun 95	n/a	Cornerstones of Information Warfare	Hierarchical: specific IW information and guidance
13	1 Oct 95	AFPD 14-1	Air Force Policy Directive 14-1, Intelligence, Air Force Intelligence Planning and Operations	Hierarchical: specific IW related guidance
14	96	n/a	The International Legal Implications of Information Warfare	Academic: specific IW commentary
15	96	n/a	Information Warfare: The Next Major Change in Military Strategies and Operational Planning	Academic: specific IW commentary
16	96	n/a	Strategic Information Warfare: A New Face of War	Academic: specific IW research
17	96	RAND IP-149	Information War and the Air Force: Wave of the Future? Current Fad?	Academic: specific IW research
18	96	RAND MR-789-OSD	The Advent of Netwar	Academic: specific IW research
19	96	n/a	Security in Cyberspace: Challenges for Society, Proceedings of an	Academic: specific IW related guidance

			International Conference	
20	96	n/a	Information Warfare (USAF)	Hierarchical: specific IW information and guidance
21	96	n/a	Information Warfare, A Strategy for Peace, The Decisive Edge in War	Hierarchical: specific joint IW guidance
22	Feb 96	n/a	A National Security Strategy of Engagement and Enlargement	Hierarchical: National Security guidance
23	7 Feb 96	JP 3-13.1	Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare C2W	Hierarchical: specific Joint IW related guidance
24	8 Feb 96	OMB Cir. A-130	Office of Management and Budget Circular No. A-130	Hierarchical: general IW related guidance
25	1 Apr 96	n/a	Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach	Academic: specific IW research
26	1 Apr 96	n/a	The Need For a USAF Information Warfare (IW) Strategy For Military Operations Other Than War MOOTW	Academic: specific IW research
27	1 Apr 96	n/a	Information Warfare in a Joint and National Context	Academic: specific IW research
28	15 Apr 96	n/a	Information Warfare and the Lack of a U.S. National Policy	Academic: specific IW research
29	May 96	GAO/AIM D-96-84	Information Security: Computer Attacks at Department of Defense Pose Increasing Risks	Academic: specific IW study
30	1 May 96	AFDD 50	Air Force Doctrine Document 50, Intelligence	Hierarchical: specific IW related guidance
31	31 May 96	CJCSI 6510.01A	Chairman of the Joint Chiefs of Staff Instruction 6510.01A, Defensive Information Warfare Implementation	Hierarchical: specific joint IW guidance
32	Jun 96	n/a	Assessments Necessary in Coming To Terms with Information Warfare	Academic: specific IW commentary
33	4 Jul 96	SAIC TNSO No. MDA903-93-D-0019	Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Ed. (SAIC)	Academic: specific IW study, information and guidance
34	15 Jul 96	EO 13010	Executive Order 13010, Critical Infrastructure Protection	Hierarchical: general IW related guidance
35	27 Aug 96	FM 100-6	Field Manual No. 100-6 Information Operations	Hierarchical: specific IW guidance
36	Oct 96	n/a	From Hackers to Projectors of Power, Information Warfare	Academic: specific IW commentary
37	Nov 96	n/a	Global Engagement: A Vision for the 21st Century Air Force (AFCS)	Hierarchical: National Security guidance

38	25 Nov 96	n/a	Report of the Defense Science Board Task Force on Information Warfare	Academic: specific IW study (OSD/AQ)
39	1 Dec 96	AFPD 33-2	Air Force Policy Directive 33-2, Information Protection	Hierarchical: specific IW guidance
40	97	n/a	Air Force Long Range Plan 1997	Hierarchical: strategic Air Force guidance
41	Apr 97	CSAP CONOPS (draft v4)	Computer Security Assistance Program Concept of Operations	Hierarchical: specific IW guidance AIA/AFIWC
42	May 97	n/a	A National Strategy for a New Century (NSC)	Hierarchical: National Security guidance
43	9 May 97	AFDD 2-5 (draft 3)	Air Force Doctrine Document 2-5, Information Operations	Hierarchical: specific IW guidance
44	Jun 97	JP 3-13 (draft 2)	Joint publication 3-13, Joint Doctrine for Information Operations	Hierarchical: joint IW guidance
45	24 Jun 97	AFDD 1 (final draft)	Air Force Doctrine Document 1, Air Force Basic Doctrine	Hierarchical: specific IW and doctrine guidance
46	15 Jul 97	n/a	Joint Doctrine Capstone & Keystone Primer (CJCS)	Hierarchical: joint doctrine guidance

The chronology established in Table 1 provides a time-scaled view of unclassified literature relevant to IO/IW strategy, and doctrine and policy formation.

The next section discusses the contribution each document makes from its respective vantage-point.

A Categorical Discussion of Key IO and IW Doctrine and Policy Guidance

The two main categories of literature are Hierarchical, and Academic. The embodiment of each of the two categories is first presented in a table, followed by a discussion of their respective documents. Each of the documents reviewed was analyzed for its specific contribution to Air Force IO and IW strategy, doctrine, and policy formation.

Hierarchical Literature. Table 2 contains a list of the Hierarchical literature, re-ordered from Table 1 in descending order, from a national security guidance level to the sub-service guidance level. Following Table 2 begins the discussion of each document.

Table 2. Key Hierarchical IO/IW Policy and Doctrine Guidance

#	Date	Long Title
34	15 Jul 96	Executive Order 13010, Critical Infrastructure Protection
24	8 Feb 96	OMB Circular A-130
42	May 97	A National Strategy for a New Century
22	Feb 96	A National Security Strategy of Engagement and Enlargement
7	95	National Military Strategy of the United States of America
4	95	Joint Vision 2010, America's Military Preparing for Tomorrow
46	15 Jul 97	Joint Doctrine Capstone & Keystone Primer
21	96	Information Warfare, A Strategy for Peace, The Decisive Edge in War
9	10 Jan 95	Joint Publication 1, Joint Warfare of the Armed Forces of the United States
11	30 May 95	Joint Publication 6, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations
44	Jun 97	Joint publication 3-13, Joint Doctrine for Information Operations
23	7 Feb 96	Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare C2W
31	31 May 96	Chairman of the Joint Chiefs of Staff Instruction 6510.01A, Defensive Information Warfare Implementation
37	Nov 96	Global Engagement: A Vision for the 21st Century Air Force
40	97	Air Force Long Range Plan 1997
20	96	Information Warfare (USAF)
12	Jun 95	Cornerstones of Information Warfare
8	95	USAF Fact Sheet 95-20, Information Warfare
1	Mar 92	AFM 1-1, Basic Aerospace Doctrine of the United States Air Force
45	24 Jun 97	Air Force Doctrine Document 1, Air Force Basic Doctrine
43	9 May 97	Air Force Doctrine Document 2-5, Information Operations
30	1 May 96	Air Force Doctrine Document 50, Intelligence
2	12 Aug 93	Air Force Policy Directive 10-7, Operations, Command and Control Warfare
13	1 Oct 95	Air Force Policy Directive 14-1, Air Force Intelligence Planning and Operations
39	1 Dec 96	Air Force Policy Directive 33-2, Information Protection
41	Apr 97	Computer Security Assistance Program Concept of Operations
35	27 Aug 96	(USA) Field Manual No. 100-6 Information Operations

Executive Order 13010, Critical Infrastructure Protection states

> certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). (1)

Information Infrastructures are an essential part of the critical infrastructures discussed in EO 13010. Although general and seemingly only remotely related to IW strategic, and doctrinal planning, EO 13010 is important, as all infrastructures are inter-related, especially the information infrastructures identified in Figure 1. Key Information Infrastructures Model. This order established the President's Commission on Critical Infrastructure Protection to study vulnerabilities and necessary policy requirements for critical infrastructure protection.

OMB Circular A-130 requires that managers implement and maintain programs to assure adequate security is provided for all information. Adequate security means "security commensurate with the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of information" (paragraph 8.b.11).

A National Strategy for a New Century comes from President Clinton and the National Security Council. It sets forth a national security strategy to advance our national interests. It states that intrusions into our critical information infrastructures

require far-reaching cooperation among the agencies of our government as well as with other nations. It also states that the U.S. military must be prepared to successfully conduct multiple concurrent operations worldwide, in the face of challenges such as information operations, and the threat or use of weapons of mass destruction. It states that because of our dominance in the conventional military arena, adversaries who challenge the United States are likely to do so using asymmetric means, such as weapons of mass destruction, information operations or terrorism. It states that the national security posture of the United States is increasingly dependent on our information infrastructures, and that these infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. It asserts that concepts and technologies are being developed and employed to protect and defend against these vulnerabilities and that we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.

A National Security Strategy of Engagement and Enlargement comes from President Clinton. It states that producers of intelligence information must form stronger relationships with intelligence product users, and help identify emerging threats to modern information systems and support the development of protection strategies (35). This indicates top level support of an intelligence role in IW strategic planning. More significantly, this document is the driving force behind the national military strategy that is discussed next.

The **National Military Strategy of the United States of America** describes the objectives, concepts, tasks, and capabilities needed in the near term by the Armed Forces

to meet our national objectives as outlined in the President's National Security Strategy of Engagement and Enlargement (i). One of the main national military objectives is to Thwart Aggression (5). This is to be accomplished through a strategy of Overseas Presence and Power Projection. Winning the "Information War" is outlined as one of the key components of this strategy (15). This component calls for the Services to have "fused information systems", and the development of new doctrine, training and control programs (15).

Joint Vision 2010, America's Military Preparing for Tomorrow provides a "conceptual template" for effective future joint warfighting by taking advantage of personnel skills and technological advances (1). The document states "we must have information superiority: the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." It also states that information superiority will require both offensive and defensive IW capabilities (16). Included in offensive IW are precision attack to destroy an enemy's command and control capability, and "electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision-makers" (16). Defensive IW is referred to as the ability to protect our ability to conduct information operations through physical security, encryption, anti-virus protection, and secure data transmission (16). Information Superiority is described as the basis for four emerging operational concepts (19):

1. Dominant Maneuver
2. Precision Engagement
3. Focused Logistics

4. Full-Dimensional Protection

This document points out the criticality of doctrine in turning the four emerging concepts into capabilities (27). Joint doctrine is stated as being both the "foundation" and "critical ingredient" for success in changing the way we prepare for and fight future wars (29). "Joint doctrine must "articulate the process", and "be flexible enough to serve as a broad framework" for use in multinational operations (29).

The **Joint Doctrine Capstone & Keystone Primer** provides an overview of selected Joint Publications. It also discusses military aspects of IW in Appendix A. Appendix A acknowledges the DII, NII, and GII, and points out that they are "inextricably intertwined." (A-48). It also states that although the word "warfare" is used in the term IW, it should not be interpreted to mean that IW is limited to military conflict alone, "declared or otherwise." (A-48).

Information Warfare, A Strategy for Peace, The Decisive Edge in War was written to provide a common framework for IW in joint operations. It outlines IW objectives at the strategic, operational and tactical levels. The strategic objectives include; Deter War, Affect Infrastructure, Disrupt Weapons of Mass Destruction Program, Support Peace Operations. The Operational objectives of IW include; Protect Global Command and Control System, Expose Enemy Deception, and Decapitate Enemy National Command Authorities/Military Commanders from Forces. The Tactical objectives include; Disintegrate Integrated Air Defense System, and Destroy/Degrade Tactical Command and Control (6). The document states that Joint IW doctrine will cover organizational responsibilities, coordination between levels of command, IW

planning considerations, integration and deconfliction of IW activities, and intelligence support to IW (17). It also states that IW doctrine will expand upon the principles of Joint Publication (JP) 3-13.1, Joint Doctrine for Command and Control Warfare (17). It highlights that IW policy is still being formed with Joint Staff participation, and that Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, Joint Information Warfare Policy, and CJCSI 6510.01A, Defensive Information Warfare Implementation are "consistent with those efforts" (16-17). CJCSI 3210.01 is classified secret and not reviewed. CJCSI 6510.01A is reviewed later in this section, as is JP 3-13.1.

Joint Publication 1, Joint Warfare of the Armed Forces of the United States is a doctrine publication that the CJCS states "establishes the foundation of our ability to fight as a joint team" (iv). He also state that all commanders must understand, teach, apply and promote the use of joint doctrine at every opportunity (iv). This document refers to doctrine as authoritative, dealing with the issue of how to employ the national military power to achieve strategic ends, which cannot be achieved as well through policy nor strategy (vi). It states that the joint campaign should "fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced U.S. technologies provide our forces" (IV-9).

Joint Publication 6, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations discusses the critical role information plays in joint warfighting. It states that C4 systems are the Joint Forces Commander's (JFC) principal tool for collecting, processing, transporting, and protecting

data and information (vii). The JFC controls the command and control support system (C2S) to ensure that data and information get to the right place, on time and in a form that is usable, which in sum generates appropriate actions (vii). As part of their responsibilities, each military service is required to provide interoperable and compatible C4 systems including personnel training and equipment maintenance (xi).

Joint Publication 3-13, Joint Doctrine for Information Operations is currently in its second draft form. It provides the overarching operational guidance for IO in the joint context (i). It discusses offensive and defensive IO principles, and describes responsibilities for planning, coordinating, integrating, and de-conflicting joint IO (i). It describes IO as actions taken to affect an adversary's information and information systems while defending one's own information and information systems, and states that IO apply across all phases of an operation and the range of military operations, and at every level of war (I-1).

It also describes IO as an integrating strategy that focuses on the vulnerabilities and opportunities presented by the increasing dependence of the U.S. and its adversaries on information and information systems (I-3). It states that in the DOD, the ultimate strategic objective of offensive IO is to affect a human decision maker to the degree that an adversary will cease actions threatening to U.S. national security interests (I-3). It also states the IO can make an important contribution to defusing crises by reducing the period of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts, thus forestalling or eliminating the need to employ forces in a combat

situation (I-4). It discusses the CJCS specific IO policy and guidance as set forth in CJCSI 3210.01A including the following:

1. Offensive IO capabilities will be employed to achieve mission objectives when deemed appropriate (I-6).

2. Information, information systems, and information-based processes (such as C2, communications, and weapons systems) used by U.S. military forces will be protected relative to the value of the information they contain and the risks associated with their compromise or loss of access. The value of information may change in relation to the objectives during peace, crisis, war, or post-conflict, as well as during the various phases of an operation (I-6).

3. Intelligence requirements for IO capabilities will be articulated with sufficient specificity to the appropriate intelligence production center (I-7).

4. Technology that affects an adversary's information and information systems and protects and defends friendly information and information systems will be pursued at every opportunity to ensure greatest return on investment (I-7).

5. Joint and Service school curricula will ensure personnel are educated in the concepts of IO in peace and IW during crisis and conflict, to include an appreciation of the vulnerabilities inherent in their information systems and the opportunities found in adversary systems. Combatant commands and Services will integrate IO into exercises to enhance overall joint operational readiness (I-7).

6. Combatant commanders will incorporate offensive and defensive IO concepts into deliberate and crisis action planning to accomplish their assigned missions (I-7).

7. The growth in IO-related technology and capabilities, and associated legal issues, make it critical for all levels of command to involve their staff judge advocate in IO policy development and employment of IO capabilities (I-8).

The preceding policy and guidance statements address some of the less-explored issues from an authoritative approach. JP 3-13 also discusses responsibilities of key IO individuals including CJCS, Chiefs of the Services, directors of the National Security

Agency, Defense Intelligence Agency, Defense Information Systems Agency, Joint Command and Control Warfare Center, and the Commander of the Joint Warfighting Center. It provides definitions and concepts that it describes as critical to understanding the entire publication (I-17). These include:

> **Computer network attack** is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. (I-18)
>
> **Information** is defined as facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation. The same information may convey different messages to different recipients and thereby provide "mixed signals" to information gatherers and users, to include the intelligence community. (I-18)
>
> **Information assurance** is defined as IO that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (I-18)
>
> **Information-based processes** are processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. Information-based processes may be found in any facet of military operations from combat through combat support and combat service support across the range of military operations, and in other elements of national power. Information-based processes are included in all systems and components thereof that require facts, data, or instructions in any medium or form to perform designated functions or provide anticipated services. For purposes of IO, examples range from strategic reconnaissance systems, to a local traffic control point in an austere overseas joint operations area (JOA), to a key adversary decision maker. (I-19)
>
> The **information environment** is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself. (I-19)

Information Operations means actions taken to affect adversary information, and information systems, while defending one's own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. IO are conducted through the integration of many capabilities and related activities. Major IO capabilities include, but are not limited to, OPSEC, PSYOP, military deception, EW, physical destruction, and computer network attack (CNA). IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities. There are two major subdivisions within IO: offensive and defensive. (I-19):

> 1) **Offensive IO** involve the integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, OPSEC, military deception, PSYOP, EW, and physical destruction, and could include CNA. (I-20)
>
> 2) **Defensive IO** comprise a process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance (IA), physical security, counter-deception, counter-PSYOP, counterintelligence (CI), electronic protection (EP), and special information operations (SIO). Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO also can support the defensive IO process. (I-21)

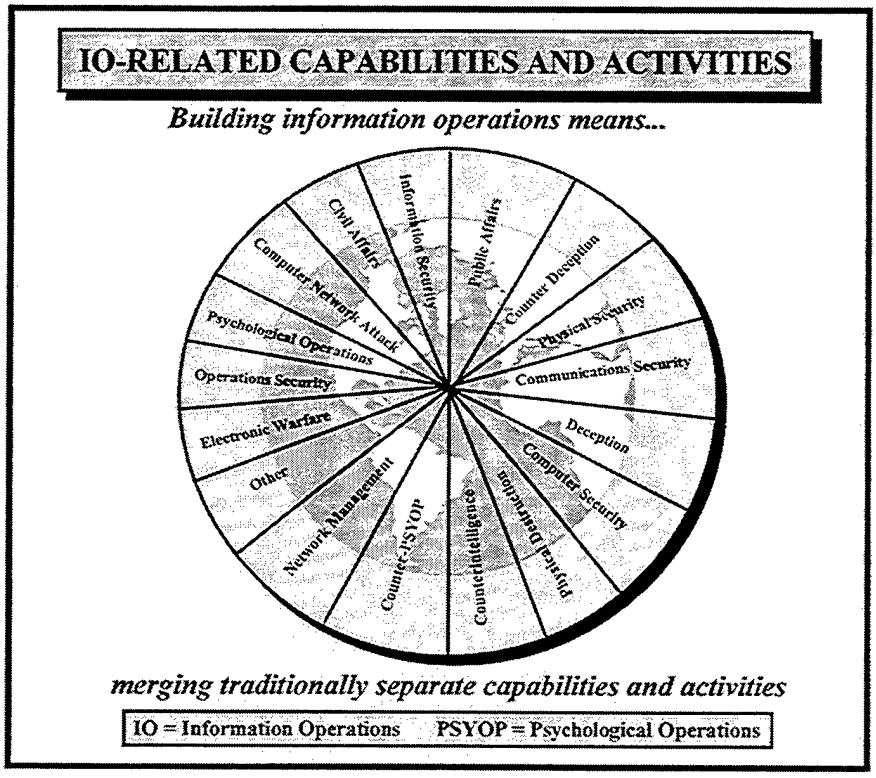
Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority may be all pervasive in the area of responsibility (AOR)/JOA, or it may be function- or aspect-specific, localized, and temporal. (I-21)

An **information system** is the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The information system also includes the information-based processes or sub-processes. (I-21)

Information warfare is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (I-21)

SIO are IO that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the US, require a special review and approval process. (I-22)

JP 3-13 graphically depicts the major capabilities and activities that make up IO. Figure 6. IO-Related Capabilities and Activities comes from JP 3-13 and is presented below.



(Adapted from JP 3-13, page I-20, Figure I-3, OI-Related Capabilities and Activities)

Figure 6. IO-Related Capabilities and Activities

In describing information environments, JP 3-13 states that the labels placed on information systems and associated networks may be misleading as there are no fixed

boundaries in the information environment, and that open and interconnected systems are coalescing into the rapidly expanding GII, NII and the DOD DII (I-25). It also provides definitions for each of these environments.

> The GII is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The GII includes more than just the physical facilities used to store, process, and display information. The personnel who make decisions and handle the transmitted information constitute a critical component of the GII. (I-26)
>
> The NII is similar in nature and purpose to the GII but relates in scope only to a national information environment. (I-26)
>
> The DII is embedded within and deeply integrated into the NII. Their seamless relationship makes distinguishing between them impossible. The DII is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The DII connects DOD mission support, C2, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network. It includes C2, tactical, intelligence, and commercial communications systems used to transmit DOD information. (I-26)

JP 3-13 describes IO targets, how they are determined, and how IO threats are defined. It states that IO targets are determined by the JFC's objectives and operations concepts and are influenced by intelligence analysis (I-29). Examples of targets include key leadership personnel, communications links, weapons systems, military or civil infrastructures, and the populace (I-30). It states that an IO threat should be defined in

terms of a specific adversary intent, capability, and opportunity to adversely influence the elements of the friendly information environment critical to achieving objectives (I-31). An IO threat must be organized, politically sponsored/motivated and have resources (I-31). Without the above criteria, hackers, criminals and organized crime, insiders, industrial and economic espionage, and some terrorists, do not constitute an IO threat, however they do fall into the general threat category that requires monitoring for indications that may tie them to such criteria (I-31).

It describes offensive IO in terms of strategic, operational and tactical objectives from peace to war. These objectives are described below.

1. Strategic: deter war, affect infrastructure, disrupt weapons of mass destruction and research and development programs, support peace operations, protect the Global Command and Control System,

2. Operational: expose enemy deception, decapitate enemy national command authorities and military commanders and separate them from forces,

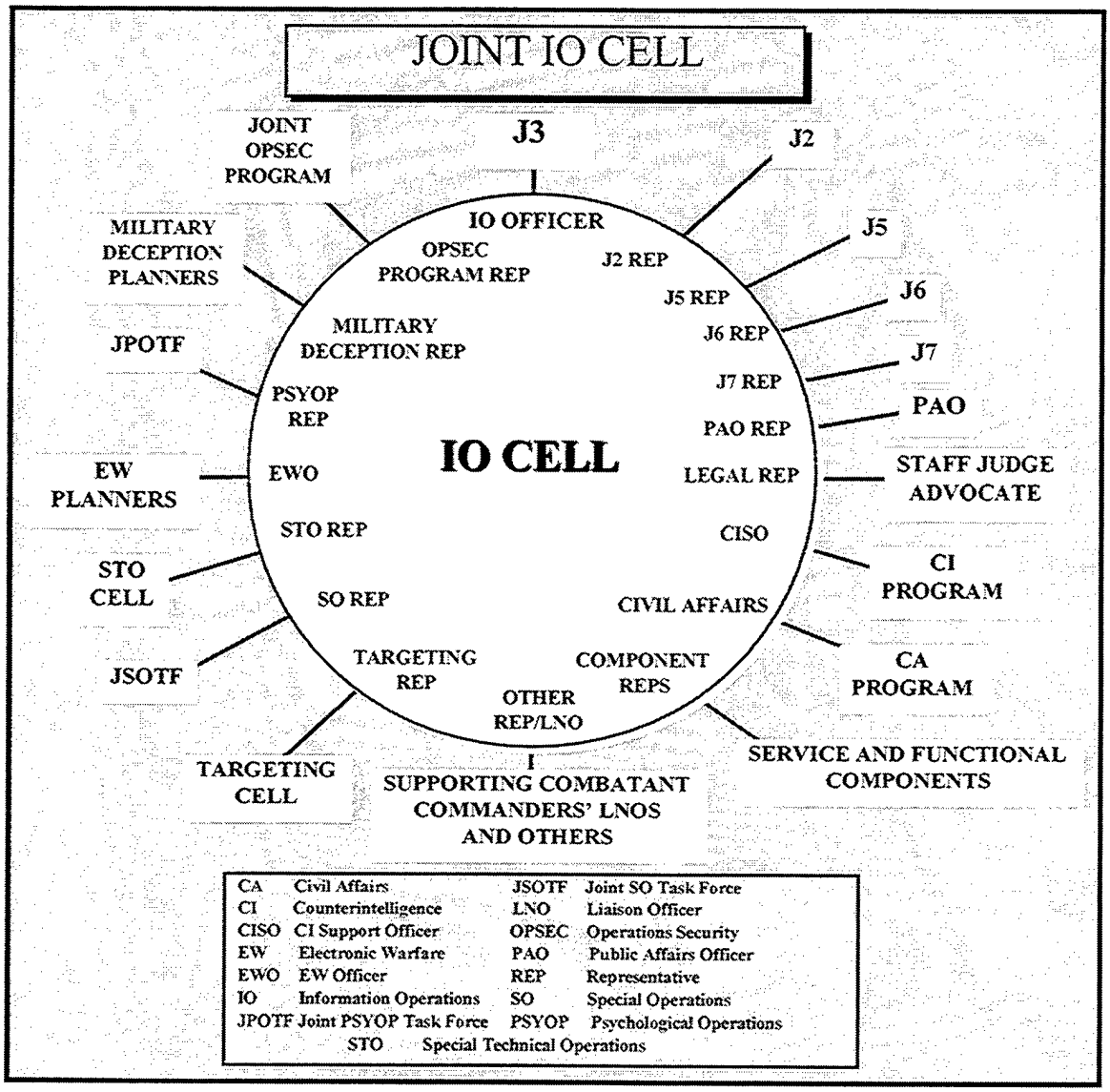
3. Tactical: disintegrate Integrated Air Defense System, destroy/degrade tactical command and control (II-2).

It also states that IO may be conducted in all types of Military Operations Other Than War (MOOTW), including disruption of drug cartel communications lines in support of drug interdiction, and conducting PSYOP against a belligerent's potential allies to attempt to severe sources of military, economic, and political support (II-16).

It describes defensive IO as being comprised of four interrelated processes including information environment protection, attack detection, capability restoration, and attack response (III-1). Defensive IO is discussed further in the review of Chairman

of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01A, Defensive Information Warfare Implementation.

JP 3-13 discusses the concept of an IO cell, which develops and promulgates guidance and plans for IO to components and supporting organizations (IV-1). The IO cell is formed from representatives from each staff element, component, and supporting agencies responsible for integrating IO capabilities and relater activities (IV-3). Figure 7. Example of Joint IO Cell depicts a typical Joint IO cell.



(Adapted from JP 3-13, page IV-4, Figure IV-1, Typical Joint IO Cell)

Figure 7. Example of Joint IO Cell

An IO Officer is assigned by the J3 to plan, coordinate, and integrate IO capabilities and activities among the various JFC staff, higher echelon staffs, component

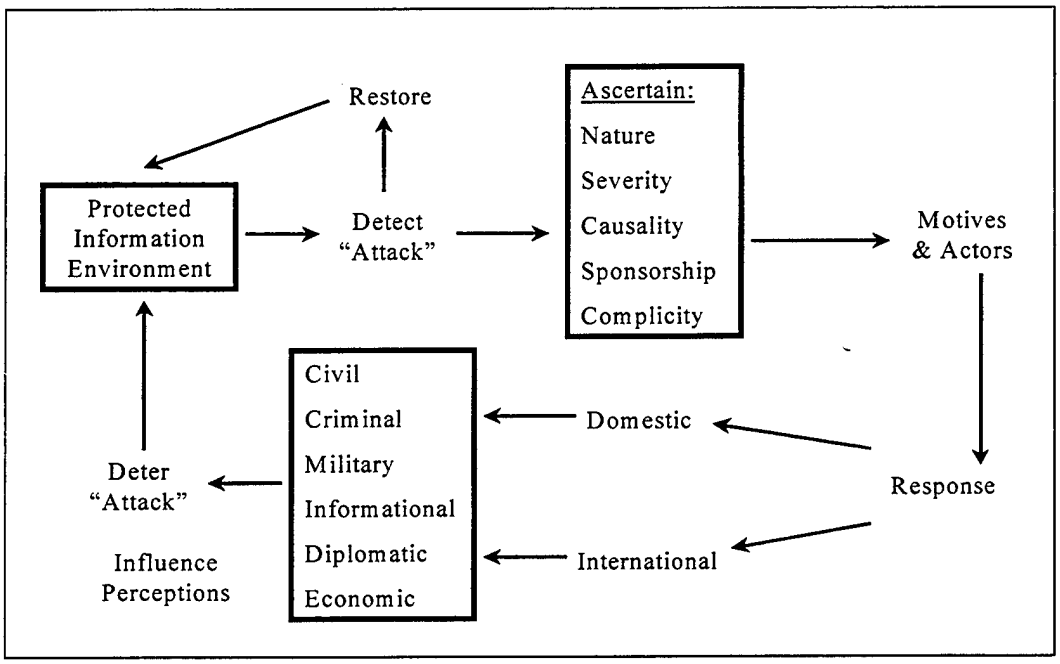
staffs, and multinational staffs (IV-5). This function is similar to that of an Executive Officer or Operations Officer on a Battlestaff or Crisis Response Element (CRE).

JP 3-13 outlines an IO planning methodology, which covers IO planning fundamentals, assessment, coordination, integration and deconfliction. Chapter VI discusses essential elements of IO training, IO in Joint exercises, and planning and exercise modeling and simulation. Appendix B contains Joint Operations Planning and Execution System (JOPES) IO guidance. The appendix and its annexes (A – G) provide logical outlines addressing military deception, electronic warfare, operations security, PSYOP, physical destruction, Public Affairs, and Civil Affairs.

Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W) states that the ultimate target of IW is the information dependent process, whether human or automated (v). C2W is an application of IW in military operations through the integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, supported by intelligence, to influence, degrade, or destroy the enemy's C2 capabilities while protecting our own from the same (v). C2W is also stated as a subset of IW (I-4). The document states that Department of Defense Directive (DODD) S-3600.1, "Information Warfare," establishes DOD policy and responsibilities for IW in DOD (I-1). DODD S-3600.1 is classified secret, and as such was not reviewed. JP 3-13.1 defines IW ultimately as "actions taken to achieve information superiority" (I-3). Information Superiority is defined as "that degree of dominance in the information domain which permits the conduct of operations without

effective opposition" (GL-8). It also states that intelligence and communications support are critical to conducting offensive and defensive IW (I-4).

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01A, Defensive Information Warfare Implementation states that the Defensive IW (IW-D) process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and information-based processes, and to defend information systems (A-1). C2 systems are a part of the information systems IW-D processes protect (A-2). The IW-D process is a combination of four inter-related processes: the information environment protection process, attack detection process, capability restoration process, and attack response process. Figure 8. IW-D Process, depicts how the larger IW-D process in implemented (A-3).



(Adapted from CJCSI 6510.01A, page A-3, Figure 2 – IW-D Process)

Figure 8. IW-D Process

The information environment protection process involves determining what to protect based on the value of the information, and how to protect via standards for protection including application of technologies and protective measures (A-4). By determining the value of information, and employing polices, procedures, technologies and operations, the Protected Information Environment depicted in Figure 8 is achieved.

The attack detection process involves the cooperation and coordination from information system developers, vendors, the Forum for Incident Response Security Team (FIRST), administrators, users, service providers, intelligence agencies, civilian and military law enforcement agencies, and those impacted by an attack in terms of reporting, responding, and initiating restoration (A-8). Essential to this process is an automated

method to assess the severity (including system damage, information compromise, and malicious logic insertion) and to mitigate these effects (A-8).

The capability restoration process relies on a pre-established prioritization scheme for restoring minimum essential capabilities (A-10). Elements of the capability restoration process may include backup and redundant links databases, alternate means of information transfer, as well as automated alerting mechanisms, post-attack system resource inventories to identify adversary implants, and post-attack vulnerability analysis for improving security (A-10). Extensive restoration needs may involve the various Computer Emergency Response Teams (CERT) available within the DOD and commercially (A-10). The attack response process involves identifying motives and actors and determining the appropriate response via domestic and/or international means. This process is designed to remove threats from the information environment (A-11).

This document assigns specific responsibilities with regard to IW and IW-D for the CJCS, the JCS, and several DOD agency directors. Each of the Service Chiefs is required to integrate IW-D concepts into Service doctrine, exercise IW-D capabilities in realistic scenarios, and conduct information security monitoring in accordance with applicable laws, executive orders, and Presidential directives (C-3).

Global Engagement: A Vision for the 21st Century Air Force was "shaped by Joint Vision 2010" to be a strategic vision addressing Air Force people, capabilities and infrastructure in order to chart the future course of the Air Force into the 21st Century (1). It states the top priority of IW as defense of our own information-intensive capabilities

(14). It points to the (Air Force) Long Range Plan for identification of "initial steps," "transition decisions," and further guidance for goal achievement (25).

The **Air Force Long Range Plan, 1997** implements Global Engagement: A Vision for the 21st Century (1). It provides directives to AF/XO for achieving Information Operations (IO) goals, and an end state of having "robust information protection for all Air Force assets, and an enhanced ability to conduct offensive IO at the tactical, operational, and strategic levels (12). The end state is to be reached through a phased program approach, and in concert with other Services and defense and national agencies and organizations (12). It specifically tasks AF/XO, AF/SC, AETC, ACC and AIA with developing education and training (including computer and network security training), and exercise programs. It tasks AIA to provide telecommunication and advanced computer defensive tool sets. AF/SC and ESC are tasked to complete Base Information Protection (BIP) at 108 locations, and to complete the remaining functions in the BIP program including boundary protection, internal controls, reconstitution and recovery, and preservation of access (13). AF/XO, SAF/AQ, and AIA are also tasked with developing additional IO tools (13).

The **Information Warfare** (USAF white paper) publish date could not be confirmed, but it is believed to have been published in 1996. It defines information warfare as any action to deny, exploit, corrupt, or destroy the enemy's information and information functions; protecting ourselves against those actions; and exploiting our own military information functions (5). This definition is consistent with the one found in Cornerstones of Information Warfare, a similar USAF white paper published in 1995. It

outlines three IW objectives: Control, Exploit, and Enhance (7). Control includes offensive and defensive counterinformation, electronic warfare, physical attack, physical defense, physical security, operations security, and counterintelligence. Exploit means operating within the realm to attain campaign objectives, such as exploiting control of information to attack the enemy, and can include psychological operations and military deception (7). Enhance means providing relevant, timely, accurate information (7). This document also states that IO "are those whose primary resource and product are information, such as weather, and command, control, communications and intelligence (7). The document commends three goals for mastering IW (15):

1. Render Air Force information and its functions, including weapon systems, secure in war and peace
2. Integrate offensive IW tools so the Air Force may conduct missions more efficiently and effectively
3. Build organizations with equipment, procedures and trained personnel prepared to plan and execute IW in support of the CINC's campaign objectives

Cornerstones of Information Warfare was the first definitive Air Force white paper on IW. It distinguishes *information age warfare* from *information warfare*, in that *information age warfare* uses information technology as a tool to conduct combat operations, while *information warfare* considers information to be a potent weapon and target unto itself (2). It considers IW important to the Air Force for two reasons (7):

1. IW offers an important means to accomplish Air Force missions
2. Widespread integration of information systems into Air Force operations makes our military information functions a valuable target

It defines Information Operations as "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces (10). The stated goal of this document is to lay out IW's doctrinal foundation to provide a sound and widely accepted basis form which current Air Force doctrine can be adapted to the Information Age (12). It suggests that IW does not fill a discrete place in Air Force doctrine, and that IW can be part of many AFM 1-1 (Basic Aerospace Doctrine of the United States Air Force) missions, with the addition of Counterinformation, C2 Attack, and Information Operations missions (13). With the addition of these three missions, the document offers the amended figure of roles and missions of aerospace power depicted below in Figure 9. Roles and Missions of Aerospace Power (10). The new missions are in bold font.

ROLES AND MISSIONS OF AEROSPACE POWER			
AEROSPACE CONTROL	FORCE APPLICATION	FORCE ENHANCEMENT	FORCE SUPPORT
COUNTERAIR	STRATEGIC ATTACK	AIRLIFT	BASE OPS & DEFENSE
COUNTERSPACE	INTERDICTION	AIR REFUELING	LOGISITCS
COUNTER-INFORMATION	CLOSE AIR SUPPORT	SPACELIFT	COMBAT SUPPORT
	C2 ATTACK	SPECIAL OPERATIONS	ON-ORBIT SUPPORT
		INFORMATION OPERATIONS	

(Adapted from Cornerstones of Information Warfare, page 10)

Figure 9. Roles and Missions of Aerospace Power

USAF Fact Sheet 95-20, Information Warfare was published in November of 1995. It highlights the three new missions identified in Cornerstones of Information Warfare: Counterinformation, C2 Attack, and Information Operations (2). In a figure depicting proposed Air Force doctrine, it expands Information Operations to include: Surveillance, Reconnaissance, Command and Control, Intelligence, Communications, Combat Identification, Precision Navigation, and Weather (3). Figure 10. Proposed Air Force Doctrine was developed from fact sheet 95-20.

PROPOSED AIR FORCE DOCTRINE			
Aerospace Control	Force Application	Force Enhancement	Force Support
Counterair	Strategic Attack	Airlift	Base Operability and Defense
Counterspace	Interdiction	Air Refueling	Logistics
Counterinformation	Close Air Support	Spacelift	Combat Support
	Command and Control Attack	Special Operations	On-Orbit Support
		Information Operations	
Surveillance	**Command and Control**	**Communications**	**Combat Identification**
Reconnaissance	**Intelligence**	**Weather**	**Precision Navigation**

(Adapted from Air Force Fact Sheet 95-20, Information Warfare)

Figure 10. Proposed Air Force Doctrine

AFM 1-1, Basic Aerospace Doctrine of the United States Air Force (Volume I) was published in March 1992 and was replaced by AFDD 1, *Air Force Basic Doctrine* during the drafting of this thesis. In the Forward, General McPeak, (Air Force Chief of

Staff when it was published) states that it is "one of the most important documents ever published by the United States Air Force" (v). He describes the two-volume set as being "at the heart of the profession of arms for airman", and that he expects every airman, noncommissioned and commissioned officer to read and study it, and be conversant with (volume II) (v). In the Introduction to Volume I, aerospace doctrine is defined as "what we hold true about aerospace power and the best way to do the job in the Air Force (vii). Doctrine is described as "a guide for the exercise of professional judgment rather than a set of rules to be followed blindly," and as something that should be alive, growing, evolving, and maturing. It states that new experiences, reinterpretations of former experiences, advances in technology, changes in threats, and cultural changes can all require alterations to parts of our doctrine even as other parts remain constant (vii).

Although IW appears nowhere in this document, the realization is that it can be woven in to our current roles and missions. The need to alter parts of the doctrine to reflect needed changes brought about by new experiences, advances in technology and changes in threats is well understood. These changes are underway as depicted by Figure 3. Current and Pending Air Force Doctrine Documents.

Air Force Doctrine Document 1, Air Force Basic Doctrine directly addresses the doctrinal implications of IW, and specifically acknowledges information systems and information technology as key warfighting factors. It describes levels of air and space doctrine in terms of basic, operational and tactical doctrine. Basic doctrine, as contained in AFDD 1, is the foundation, and states the fundamental beliefs that describe and guide proper use of air and space power (4). Operational doctrine, contained in the AFDD 2

series (including AFDD 2-5 Information Operations), describes the organization of air and space forces, and applies the principles of basic doctrine to military actions (4). Tactical doctrine describes the proper use of weapons systems, both individually and collectively to accomplish specific objectives (4). AFDD 1 also describes three types of doctrine: Service, Joint, and Multinational. Service doctrine outlines each Service's competencies, and provides guidance for force application (4). Joint doctrine provides guidance for integrating Service competencies in joint operations (4). Multinational doctrine, similar to Joint doctrine, describes how to integrate U.S. forces with allies in coalition warfare (4). These levels and types of doctrine provide a framework for thought and decision making for all levels of warfighters.

AFDD 1 states that in addition to the media of air, land, sea, and space, *information* is another medium in which warfare can be conducted (7). It states that the U.S. Air Force conducts air, space, and information warfare to support the objectives of joint force commanders (JFC) (7).

AFDD 1 also discusses IW as it applies to the principles of war. It states that due to the versatility of air and space forces, the principle of *objective* is especially important in air, space, and information warfare (10). In discussing the principle of *mass*, AFDD 1 suggests that mass is an effect, rather than just overwhelming quantity, and that air, space, and information forces together have altered the concept of massed forces (12). It gives an example of past massed forces including hundreds of planes used to attack two major targets each day, versus the use today of a single precision weapon to exact the same effect (12). In discussing the principle of *security*, AFDD 1 states that security from

enemy intrusion conceals our capabilities and intentions, at the same time allowing friendly forces to gather information on the adversary (13). It states that air and space power includes information power, not just aircraft, missiles and satellites, and that understanding this idea is critical to security (13). It also states that information has always been a part of air, land, and sea warfare, and that the proliferation of information technologies has made information more central a figure to the outcome of a conflict (13).

AFDD 1 discusses information superiority as a validated concept citing precise strategic attacks against Iraq's central command and control structure during Desert Storm as an example (14). It also discusses the strategic value of information technology in the following paragraph:

> Additionally, information technology can directly or indirectly affect national or group leadership, population, and infrastructure bypassing direct military confrontation. Whoever now has the best ability to gather, understand, control, and exploit information, and deny the same capabilities to an opponent, has a distinct strategic advantage. (14)

It discusses the role of information as applied to the principle of *surprise* stating that intelligence and space systems enhance the ability to achieve surprise by providing information superiority through reconnaissance, surveillance, and communications (14). AFDD 1 further discusses the role of information as is applies to the tenets of air and space power; which are more specific than the principles of war (15). One tenet, that air, space, and information forces produce synergistic effects, suggests that coordinated air, space and information forces can collectively produce effects that exceed those that could

be attained through the separate use of each (17). Another less obvious tenet states that air, space, and information systems are uniquely suited to persistent operations, because they do not have to occupy terrain or remain in proximity to areas of operation to bring force upon them (17). In other words, operations in the air, space, and information dimensions can allow air and space forces to visit and revisit targets almost at will (17).

AFDD 1 describes information superiority as the ability to collect, control, exploit and defend information while denying an adversary the ability to do the same, and includes gaining control over the information realm and fully exploiting military information functions (20). It also states that information superiority was the first function of the Air Force, referring to the use of balloons and airplanes as spotters for Army commanders (20). A more recent example is also given in that information superiority (through the use of air- and space-based surveillance and reconnaissance) enabled the U.S. to rapidly respond to the Iraqi force build-up that threatened Kuwait in October 1994 (21).

AFDD 1 states that one of a commander's primary tasks is to gain and maintain information superiority with the objective of achieving faster and more effective command and control of forces than the adversary (21). It states that the main goal of information superiority is to have information that is accurate, usable, and not overwhelming, and information that enables one to consistently react to a situation and make accurate decisions more rapidly than the enemy (21). It suggests that dominating the information spectrum may improve the speed and quality of our observe-orient-

decide-act (OODA) loop, and also degrade the enemy's; affecting his perception of the situation and available courses of action (21).

AFDD 1 ties the U.S. Air Force's core competencies to Joint Vision 2010's Full Spectrum Dominance and states that the operational concepts of Joint Vision 2010, (Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection), are enhanced by information superiority and technological innovations (26).

AFDD 1 states that Information Operations are actions taken to affect adversary information and information systems while defending one's own information and information systems, and that information warfare is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary (30). It states that methods used to achieve information warfare objectives include electronic warfare, psychological operations, military deception, physical attack by air and space forces, information attack by electronic means, and application of various security means (30).

AFDD 1 lists Counterinformation as one of the basic functions of air and space power (31). Counterinformation is described as having control of the information realm to establish information superiority in an environment where friendly forces can conduct operations without suffering substantial losses, while at the same time denying the enemy to conduct their operations; thus preventing the enemy from achieving an information advantage (36). Counterinformation has both offensive and defensive components. Offensive counterinformation consists of operations designed to destroy, degrade, or limit enemy information capabilities in order to control the information environment (36).

Defensive counterinformation includes operations security, information security and counterintelligence designed to assess and reduce the threat of unintentional and unwanted release of information (36).

AFDD 1 states that it is intended to be the lead publication in the Air Force doctrine hierarchy and the premier statement of the "theory" that guides the employment of Air Force air and space power (50). It also describes itself as a work in progress, and that none of the Air Force doctrine documents will be complete, (implying to the need to regularly revise doctrine based on learning experiences, and to exploit new ideas and technologies) (50).

Air Force Doctrine Document 2-5, Information Operations is divided into six chapters which discuss the nature of information operations, information warfare, peacetime information protect programs, IW support to theater operations, information protect response to domestic IW emergencies, and implications for IW. AFDD 2-5 states that IW is a subset of Information Operations (IO) and acknowledges the "information battlespace" as a fifth dimension in addition to air, land, sea, and space; where a nation strives to achieve an advantage over its adversaries (1). It states that information superiority is the one Air Force core competency on which all other core competencies rely (2). It also states that the future joint (forces) team will rely heavily on a robust command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) architecture to maintain information superiority (2). AFDD 2-5 states that IW has both offensive and defensive components and that IW is IO conducted primarily during time of crisis or conflict to achieve information superiority (3).

It defines Information Assurance (IA) as an evolved form of Information Protection, consisting of measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation (ability to confirm source of transmission and data) (3). IA is designed to protect IO (3).

AFDD 2-5 states that the goal of IW is to achieve an information advantage (5). It states that IW targets decisions by affecting the flow of information to and from the decision maker (5). AFDD 2-5 describes IW as consisting of offensive and defensive counterinformation, and information enhancement (5). Offensive counterinformation (OCI) includes psychological operations, electronic warfare, (military) deception, computer network attack (CNA)/information attack, and physical destruction (5). Defensive counterinformation (DCI) includes IA, counter-deception, counter-psychological operations, and counter-intelligence (5). Information enhancement includes operations and information systems that enhance force effectiveness in the areas of intelligence, command and control, precision navigation and positioning, surveillance and reconnaissance, and weather (5). Command and control warfare (C2W) is described as a subset of IW, in that it specifically aims at attacking and defending command and control targets (5).

AFDD 2-5 states that the Air Force Computer Emergency Response Team (AFCERT) is the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities (25). Using Air Force Information Warfare Center (AFIWC) personnel, the AFCERT coordinates technical resources to

assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities (25). In discussing IW support to theater operations, AFDD 2-5 describes the role of IW Squadron (IWS) activities in support of theater operations.

> An IWS is configured with advanced systems and tools, similar to those found within the AFCERT. Linked to the AFCERT, the IWS depends on the AFCERT systems and data bases for pull-on-demand theater support as well as push-oriented Indications and Warning (I&W), intelligence, and mission planning support—much of which is automated. (27)

The IWS supports information assurance operations by deploying augmentation forces to the operations theater (27). These forces support both base and deployed network control centers and other organizations that rely on IWS capabilities (27). Another area of IW support to theater operations is IW targeting. IW planners recommend strategic and air-related targets by first following universal and self-imposed guidance, including legal and political guidelines, and then selecting targets based on national, theater, and command objectives such that a maximum payoff is achieved for each given course of action (target nomination) (28). IW target nominations are integrated into attack plans and tasking orders, and eventually a Master Air Attack Plan (MAAP) (29).

Air Force Doctrine Document 50, Intelligence provides Air Force doctrine for intelligence in support of basic air and space doctrine (1). It states that intelligence is a primary contributor to information dominance in support of the Air Force concept of global awareness (2). It describes IO as including any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of

military forces (2). It describes the AFIWC as providing time-critical intelligence information 24 hours per day (6). It also states that the AFIWC is one of the Air Intelligence Agency's Centers of Excellence, and that it develops, maintains, and deploys IW and Command and Control Warfare C2W capabilities in support of operations, campaign planning, acquisition and testing (6). The AFIWC conducts battlespace preparation such as construction and maintenance of target sets for Command and Control nodal analysis, centers of gravity, and concealed facilities, and acts as a time-sensitive, single focal point for intelligence data and C2W services (7). The AFIWC also provides technical expertise for computer and communications security, and is the Air Force focal point for tactical deception and operations security training (7).

Air Force Policy Directive 10-7, Operations, Command and Control Warfare was published 12 August 1993, before most doctrine and policy regarding IW was being conceptualized. It states that the Air Force will implement procedures to control the sources of friendly information that may be exploited by adversaries (1).

Air Force Policy Directive 14-1, Air Force Intelligence Planning and Operations was revised 1 October 1995 to highlight areas not previously covered such as directing Air Force intelligence to integrate information dominance concepts and objectives into intelligence planning and resource allocation activities (1).

Air Force Policy Directive 33-2, Information Protection was revised and renamed from AFPD 33-2 C4 Systems Security. It sets forth policy to ensure that the Air Force is provided with accurate, timely and secure information in any form required, at any time and place (1). It establishes an information protection (IP) policy that calls

for information system user training to protect against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons (1). The policy also requires that acquisition managers consider IP requirements throughout the acquisition process (1).

Computer Security Assistance Program Concept of Operations also known as CSAP CONOPS is still in draft (version IV, April 1997) as of this writing. It was developed by the AFIWC Engineering Analysis Directorate. Although the CSAP CONOPS is still in draft form, the basic concepts are currently operational. The Computer Security Assistance Program (CSAP) was developed and is maintained by the AFIWC and serves as a strategy for Defensive IW, and IP operations (3). CSAP CONOPS states that although the Air Force is currently not engaged in war on land, sea, air or space, it is engaged in a cyberspace war with amateur and professional intruders who attack Air Force systems 24 hours a day (3).

The CSAP concepts came from lessons learned from the analysis of computer security incidents and computer network technology evaluations (7). The CSAP is an element of DCI, with the objective of protecting friendly Command, Control, Communications, and Computer (C4) systems (12). Specifically, the CSAP is designed to protect C4 systems against intrusion, detect attempted intrusions, and recover from successful intrusions through an integrated set of projects and programs (12).

The CSAP operating environment consists of Air Force major commands (MAJCOMs) and associated Network Control Centers (NCCs). CSAP operations include network mapping (NMAP), On-line Survey (OLS), Intrusion Detection Tools (IDT) such

as Automated Security Incident Measurement (ASIM), Incident Response (IR), Intelligence Support, and Law Enforcement via Air Force Office of Special Investigations (AFOSI) (14). NMAP is intended to establish the topology of Air Force networked computer systems (22). Such a topology is currently unknown (22). NMAP will provide a network mapping program capable of remotely collecting system identification data (22). OLS was designed to help Air Force organizations improve their security posture (22). It takes advantage of known operating system weaknesses to remotely gain access to system resources (23). The ASIM tool, one of the IDTs, monitors internet traffic (23). Specifically, it enables analysts to detect and identify unusual network events and network activity (23). IR is designed to isolate, contain, and recover from system intrusions before mission impact occurs (24). IR is a concerted effort between the AFCERT, the affected organization(s), and several other agencies (24). Intelligence Support (threat data) is provided to the CSAP by a dedicated all-source intelligence team (25). The data is disseminated to IP managers and commanders to help identify risks, set priorities, and develop countermeasures (25). CSAP law enforcement requirements are handled by the AFOSI, who control all criminal and counterintelligence operations (26).

The CSAP consists of four technical teams: Computer Security Engineering Team (CSET), Electronic Security Survey Team (ESST), Security Technology Insertion Team (STIT), Countermeasures Engineering Team (CMET), and a Program Management & Analysis Team (PMAT) (14). CSET teams conduct computer exploitation and network security monitoring on Air Force systems to detect vulnerabilities and unauthorized activities with the primary mission of testing and assessing the specific C4 system and

network security posture of a base or organization (27). ESST teams measure the effectiveness of organizational computer security by physical and electronic examination of individual workstations (PCs) (28). The ESST mission is to find vulnerabilities and recommend countermeasures, and to collect computer security posture statistics (28). The STITs mission is to enhance the security posture of Air Force networks through technical support including requirement identification, solution development, component evaluation and testing, and prototyping and fielding solutions (29). The CMET identifies and/or develops security countermeasures for computer system vulnerabilities (29). The PMAT manages the CSAP projects from a financial, contractual and marketing standpoint (32).

CSAP operations are conducted by the AFCERT (16). The AFCERT, which is operational 24 hours a day, responds to computer security incidents by:

> processing and responding to all Air Force users' or automated incident reports (of intruder and malicious logic incidents),
>
> processing and disseminating countermeasures for all reported C4 systems security vulnerabilities,
>
> reporting collected information on vulnerabilities and incidents to other potential targets and organizations, and
>
> providing updates to information protection databases. (20)

It is stated in the CSAP CONOPS that the overriding lesson learned from recent C4 system security incidents is that the fundamental weakness in the security of Air Force C4 systems is people, not technology (16).

Field Manual No. 100-6 Information Operations is the U.S. Army's capstone doctrine for Information Operations (IO) (iii). Published 27 August 1996, it remains the only service-level IW doctrine document of its kind in the field. It addresses the operational context of IO, relevant terminology, and the IO environment as they apply to all Army personnel (iii). It states that it supports the National Military Strategy, explains the fundamentals of IO for the Army, and goes beyond the joint military strategy of C2W (v). It discusses the operating environment as an expanding information domain called the Global Information Environment (GIE), a portion of which is the Military Information Environment (MIE) (1-1). The GIE includes all individuals, organizations, or systems, that collect, process, and disseminate information to national and international audiences (1-2). According to FM 100-6, the GIE includes the Global, National and Defense Information Infrastructures, as well as political leaders, media, industry, other governments and international organizations such as the Red Cross (1-2). The MIE consists of information systems and organizations (friendly and adversary), military and non-military, which support, enable or influence specific military operations (1-4). It lists sources of threats as unauthorized users, insiders, terrorists, non-state groups (drug cartels, social activists), foreign intelligence services, and political opponents or opposing militaries (1-6). It recognizes that it is difficult to analyze and determine the origins of a particular incident, and that boundaries between the threat groups are difficult to distinguish (1-6). It states that commanders and national leaders face a set of interrelated challenges in dealing with global visibility of operations in the

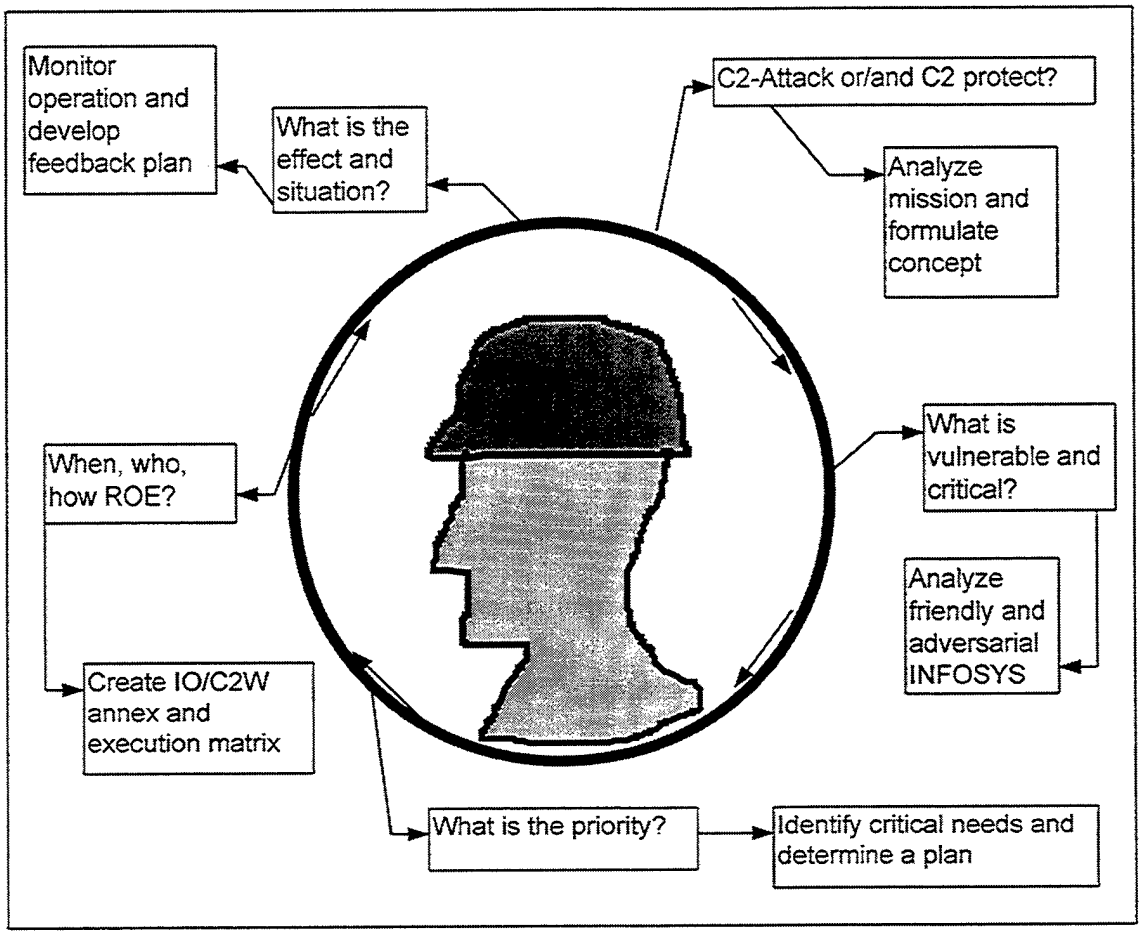
GIE including information security, conducting continuous operations, policy and public opinion, morale of the forces, and legal considerations (1-8).

In discussing strategy, FM 100-6 describes IO as the Army's interpretation of IW, and states that the Army has chosen to take a broader approach to defining IW than the DOD, to include its impact on ground operations (2-2). It states that if carefully conceived, coordinated and executed, IW will; contribute to defusing crises, reduce the period of confrontation and enhance the impact of informational, diplomatic, economic, and military efforts, and finally, forestall or eliminate the need to employ combat forces (2-2). It also states that the strategic goal of IW is to seize and maintain a decisive advantage by attacking an adversary's NII through exploitation, denial, and influence, while protecting friendly information systems (2-2).

In discussing the fundamentals of IO, FM 100-6 identifies six critical activities that it describes as essential to a sound IO program. They include acquiring, using, protecting, exploiting, denying, and managing information and information systems (2-1). These six critical activities occur within three interrelated components of IO: Information Systems, Operations, and Relevant Information and Intelligence (RII) (2-3). The Information System component consists of an architecture with horizontal and vertical integration that allows for global connectivity, and entails the migration from the Army's current Army Command and Control System (ACCS), to the Army Battle Command System (ABCS) (2-8). There are three operations used by the Army in its Operations component, to gain information dominance. These include Command and Control Warfare (C2W) to attack and protect specific targets sets, Civilian Affairs (CA) to ensure

the commander gains civilian support using liaison personnel, and Public Affairs (PA) to address the media, balancing operations security with the public's right to know (2-4), (3-0). The component of RII centers on situational awareness: the right people having the right information at the right time (2-6). Relevant information is defined as information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the current operational mission (4-0). Intelligence is the critical sub-element of relevant information that provides a commander with an accurate view of the threat situation for consideration in current and future operations (4-3). This includes understanding the adversary and the information battlespace. Intelligence must provide a commander with an understanding of the enemy's decision-making processes and direction dissemination means to subordinates (4-4). In order to determine how and where to effectively influence the enemy's actions, a commander must understand the enemy's use of information (4-4).

The activities and components of IO come together in the Army's IO planning process, which consists of five steps: mission analysis, prioritization, concept of operations, execution, and feedback (6-8—10). This process is described cyclically in terms of critical questions and methodologies as shown in Figure 11. Army IO Planning Process.



(Adapted from FM 100-6, page 6-11, Figure 6-3 IO Planning Process)

Figure 11. Army IO Planning Process

Academic Literature. Table 3 lists the Academic literature presented in the same chronological order as it was in Table 1. Following Table 3 begins a discussion of each document's contribution to IW strategy, and doctrine and policy formation.

Table 3. Key Academic IO/IW Policy and Doctrine Guidance

#	Date	Long Title
3	95	Information Warfare, Airpower Journal
5	95	New World Vistas, Air and Space Power for the 21st Century, Information Applications Volume
6	95	New World Vistas, Air and Space Power for the 21st Century, Information Technology Volume
10	1 May 95	Information Warfare: An Opportunity for Modern Warfare
14	96	The International Legal Implications of Information Warfare
15	96	Information Warfare: The Next Major Change in Military Strategies and Operational Planning
16	96	Strategic Information Warfare: A New Face of War
17	96	Information War and the Air Force: Wave of the Future? Current Fad?
18	96	The Advent of Netwar
19	96	Security in Cyberspace: Challenges for Society, Proceedings of an International Conference
25	1 Apr 96	Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach
26	1 Apr 96	The Need For a USAF Information Warfare (IW) Strategy For Military Operations Other Than War MOOTW
27	1 Apr 96	Information Warfare in a Joint and National Context
28	15 Apr 96	Information Warfare and the Lack of a U.S. National Policy
29	May 96	Information Security: Computer Attacks at Department of Defense Pose Increasing Risks
32	Jun 96	Assessments Necessary in Coming To Terms with Information Warfare
33	4 Jul 96	Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Ed. (SAIC)
36	Oct 96	From Hackers to Projectors of Power, Information Warfare
38	25 Nov 96	Report of the Defense Science Board Task Force on Information Warfare

Information Warfare, Airpower Journal was published in the Spring of 1995. Author George J. Stein describes four sets of ideas regarding IW including defining IW, developing an IW strategy, IW doctrine development based on current Air Force doctrine, and the danger of failing to develop IW (31-32). He states:

> Information warfare, in its largest sense, is simply the use of information to achieve our national objectives. (32)

He also states that IW is about ideas, and, influencing the way humans think and the way they make decisions (32). He describes IW as using information to create a substantial mismatch between the U.S. and a given adversary such that the adversary's strategy is defeated before physical combat can begin (32). He states that the target of IW is the human mind (32). He also states that although cyberspace is the IW battlefield, the battle is still for the mind (33). He discusses how television can be used as an IW tool in that it can be used to shape the political context of a conflict (33).

In discussing IW strategy development he raises questions for consideration including: What information is needed? What organizational changes would occur in the way we gather process, distribute, and use information? What information-based operational changes could then happen? (35). He suggests the idea that IW strategy be led by vision, allowing technology to follow, and offers Gen. William Mitchell's vision of airpower potential as an example (36). Stein suggests what the challenge of IW is with regard to strategy development in the following paragraph:

> Is there something about information and the information technologies that would permit us to create such a mismatch between what, when, and how we and our opponents observe, orient, decide, and act or such a level of "information dominance" that the opponent is helpless—and not just on the battlefield? Is there a way we could use information, like current theories of airpower, to create an "information campaign" that engages an opponent simultaneously in time, space, and depth across the full range of his strategic structures so that the result is strategic paralysis (he is deaf, dumb, and blind to anything except that which we permit him to hear, say, or see)? Not that we just blind him, but that he sees what we wish him to see without realizing that it's "our" reality, not his. Can we envision that kind of strategic information warfare? (37)

He argues that AFM 1-1, Basic Aerospace Doctrine of the United States Air Force could be used as a template for IW doctrine (38). He compares air warfare in the air and space realms to IW in an information realm and derives from offensive and defensive counterair, offensive and defensive counterinformation as strategies for control (38). He states that both airpower and IW are more than just force multipliers (38). He also states that a review of airpower debate history reveals that those who viewed airpower solely as a force multiplier to support the "real" effort failed to recognize its strategic potential, and that if IW doctrine heads down the same path, its potential (for exploitation of information dominance and identification and acquisition of relevant technologies) would be missed (38). He states:

> The challenge is to use Air Force doctrine as the foundation to envision the "Information Campaign" which, like the "Air Campaign" in the Gulf War, is of strategic significance. What, for example, would "speed, precision, and lethality" be in an "info-strike? (38)

Stein warns of the U.S. "being on the receiving end of an Electronic Pearl Harbor" if we fail to develop both offensive and defensive IW strategies (38). He cites the diffusion of information technology, potential opponents observing and copying our technologies and operational innovations, and adversaries taking advantage of IW as more than just a force multiplier as reasons why we should develop an IW strategy (39).

New World Vistas Study: At the direction of the Secretary of the Air Force, and the Air Force Chief of Staff, the USAF Scientific Advisory Board (SAB) was tasked to study advanced air and space ideas and project them into the future. The results of the

SAB-led work of 130 individuals from research, academia, government, and industry were published in a 15-volume set of monographs entitled New World Vistas (FIE). Two volumes, Information Applications and Information Technology discuss aspects of IW, providing recommendations and guidance with regard to technologies and concepts

New World Vistas: Information Applications Volume discusses the future of the infosphere as becoming a more powerful and useful information utility for management of the global battlespace among other things (v). It states that IW will radically alter the tasks associated with putting energy on targets and that IW will take place within the infosphere, extending beyond the military domain and become unpredictable (v). It suggests that the degree to which the Air Force develops the professional expertise to engage in national policy debates, allocates research and development expenditures, and encourages a military doctrinal evolution will determine its future (v). It warns that we should prepare ourselves for sophisticated software weapons operating solely within the infosphere, directed against our economic, social, and military institutions. It states that the Air Force should prepare itself through its research programs for a key role in dealing with protection issues (vi). It suggests that among larger nations, aerospace warfare will eventually be dominated by forces possessing the best ability to protect its information assets, while attacking those of its opponents, among other capabilities (vii). The key recommendations of the Information Applications Panel are given below:

> Primary: It should be the goal of the Air Force to achieve information dominance to enable the execution of its missions through the

unconstrained but protected use of the infosphere, including segments that the Air Force does not control.

1. Get the right knowledge, to the right place, at the right time for all aerospace missions
2. Protect all Air Force computers, software, and data regardless of platform or location, particularly those involved in warfighting
3. Achieve global communication between the air, ground, and space assets of the Air Force, as well as those with whom we operate
4. Maximize the speed and quality of Air Force coordination, planning, and execution
5. Dominate the information battlespace
6. Develop doctrine needed for the use of information in dynamic command and control of joint forces (xiv)

The Panel also recommended that the MII development be driven by IW considerations (53). It states that Information Infrastructures are emerging as centers of gravity for (trans) national power (70). It suggests that although protect and attack actions will involve and impact the private sector, a national security rather than private/commercial sector perspective must dominate strategy and policy formation (70).

In planning IW strategy, the Panel suggested that following actions should be featured (70-1):

1. Robust attack technologies capable of on-demand use against a range of target technologies/systems
2. Leveraging of intelligence community parallel technologies to access and process targets
3. Pursue long term expert based study on improving techniques for computer attack which increase on-demand effectiveness with reduced manpower investment
4. Pursuit of intelligent agents for attack mission

The Panel noted the following doctrinal implications (74):

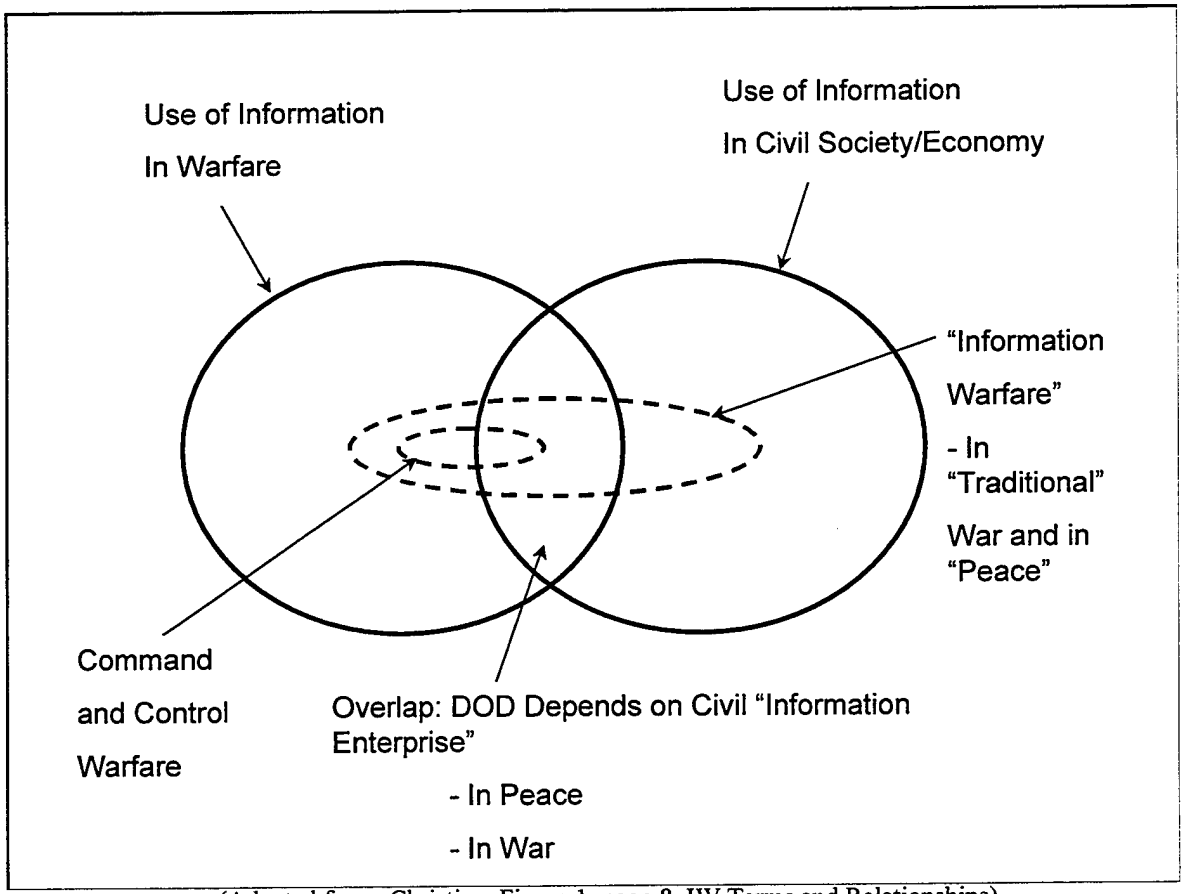
> By the 21st century, joint doctrine will center on JTF operations and will lead and integrate directly with service doctrine. Joint doctrine will drive standardized tactics, techniques, and procedures for JTFs operating across different theaters. This is a crucial step in the evolution of information in warfare as a combat multiplier, because it will place all operating elements on a common standard. Doctrine will retain its role as a guidepost (vice directive) for commanders. They will continue to tailor their planning and execution based on mission using doctrine as a standard. Joint-led doctrine will be a necessary foundation for the effective use of information in warfare technological capabilities.

The panel stated that information technology would influence doctrine in a major way; but that doctrine provided the means to apply technology smartly to military operational environments and to highlight the significant changes and seams created by the infusion of technology (79).

New World Vistas: Information Technology Volume discussed the importance of High Assurance Systems. The Information Technology Panel suggested the following:

> Existing information intensive systems are currently blatantly vulnerable. Recent studies have shown the domestic electrical power grid, financial systems, and telecommunications infrastructure to have between modest and virtually non-existent protection against information-based attacks. Yet basic techniques exist capable of deterring many of these attacks, and continued development and dissemination of known cryptologic technology will be able to provide very high levels of security to individual systems. Attention should be paid to widespread integration of such technology into Air Force software at all levels (networks, operating systems, and applications). Important attention should also be paid to Air Force policy regarding cryptology: in particular, we recommend the Air Force employ a key escrow (or similar) system, in order to ensure that the internal use of cryptographic techniques cannot provide an impenetrable wall of privacy to unauthorized action by Air Force personnel. (10)

Information Warfare: An Opportunity For Modern Warfare was co-authored by 23 students at the Air Command and Staff College at Maxwell AFB, AL. It explores strategies for integrating IW into basic aerospace doctrine, identifies gaps in IW and air power literature, and suggests approaches for addressing the gaps in current Air Force doctrine. It recognizes that IW is in essence a battlespace which must be controlled and exploited (7). The document presents a figure, which captures various aspects of, and describes the relationships of, some IW terms established as a top-level framework. The figure is presented below as Figure 12. IW Terms and Relationships.



(Adapted from: Christian, Figure 1, page 8, IW Terms and Relationships)

Figure 12. IW Terms and Relationships

In Figure 12. IW Terms and Relationships, Command and Control Warfare is the military subset of IW. This figure can easily be related to Figure 1. Key Information Infrastructures Model, which was presented in Chapter 1. Taken together, these figures demonstrate the overlapping infrastructural environment of information, and its uses in IO and IW.

The work defines IW as any action taken to deny, exploit, corrupt, or destroy the enemy's information and information systems, while protecting friendly information and information systems (7). This definition is consistent with the one found *in Cornerstones of Information Warfare*, an Air Force white paper that was reviewed earlier in this chapter. The authors present a table (Table 4 below) which shows how the IW roles and missions fit into those described in AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, as established by the office of the Deputy Chief of Staff for Operations, United States Air Force.

Table 4. Aerospace Doctrine Roles and Missions

Aerospace Control	**Force Application**	**Force Enhancement**	**Force Support**
Counterair	Strategic Attack*	Airlift	Base Ops & Defense
Counterspace	Interdiction*	Air Refueling	Logistics
Counterinformation*	Close Air Support*	Spacelift	Combat Support
	C2W*	Special Operations	On-Orbit Support
		Information Enhance*	

* Missions of Information Warfare

(Adapted from: Christian, Table 1, pg 10, Roles and Missions of Aerospace Doctrine)

The authors point out that association of IW missions with aerospace roles provides a consistent framework for aerospace doctrine (10). The descriptions for each of the IW roles identified in the table are provided below:

> **Counterinformation** has offensive and defensive aspects, like counterair. Offensive counterinformation consists of actions taken to establish control of the enemy's information systems and operations, and their information warfare resources. Defensive counterinformation consists of actions used to protect friendly information resources (from offensive counterinformation operations conducted by the enemy). (11)
>
> **Strategic Attack**, in the form of a strategic information attack, consists of attacking the enemy's information systems, which support economic, electrical, or transportation systems (12). This may include corruption, deception, flooding, delaying, denial, disruption, degradation, and destruction. (14)
>
> **Interdiction**, in the form of information interdiction includes attacking information dependent targets such as enemy communications systems. (12)
>
> **Close Air Support**, in the form of a close information attack could include electronic warfare against enemy radar in support of a tactical commander. (12)
>
> **C2W**, as a doctrinal subset of IW, consists of military information operations designed to disrupt the enemy's C2 system in order to affect their decision cycle. (12)
>
> **Information Enhance** includes reconnaissance, surveillance, command and control, precision navigation, and meteorological services to enhance overall force effectiveness. (14)

The authors present a set of refined IW goals, missions and objectives as shown on the following page in Table 5.

Table 5. Information Warfare Objectives

IW Goals	IW Missions	IW Objectives
Establish Information Dominance	Offensive Counterinformation (Control)	Establish Ability To Manipulate Enemy Information Functions
		Degrade/Destroy Enemy Offensive IW Capabilities
	Defensive Counterinformation (Protect)	Defend Friendly Information Functions From Attack Or Degradation
	Enhance	Enhance Friendly Operations By Exploiting Information Technology
Degrade Enemy Will And Capability To Fight	Attack	Degrade Enemy Will To Fight
		Disrupt Or Paralyze Enemy Decision Cycle
		Disrupt, Degrade, Or Destroy Enemy Capabilities

(Adapted from Christian,Table 4, page 117, Information Warfare Objectives)

The authors also offer a conflict resolution framework and the beginnings of a strategy-to-task analysis, which breaks out several of the IW Missions identified in Table 4 into specific tasks. They point out the need to understand the IW environment, which envelops land, sea, air and space media (16). They state that IW is conducted in the infosphere; where information is collected, processed, transmitted, stored, or used. The infosphere includes information systems, processes, transmission media, and information users (17). The authors describe the characteristics of IW as lack of restriction, stealth, non-lethality, speed, reversibility of effect and flexibility (20-23). They conclude that the Air Force should use IW to target an enemy's decision-making cycle (140). Finally, they suggest that of all the tools and concepts that have been developed for modern warfare,

IW has the greatest potential to subdue the enemy without a fight, and state that the IW campaign must be the first to be executed (149).

The International Legal Implications of Information Warfare highlights the problem of not having a concise, universally accepted definition for IW. The article presents several varying definitions of IW including those found in the Air Force's *Cornerstones of Information Warfare*, and *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, authored by Winn Schwartau (101). The author suggests that conventional bombing of a computer center constitutes IW using the Air Force's definition, but is not IW using Schwartau's or the definitions of others (101). This, the author states, complicates the legal matters involved (102). He states that, under its broadest definitions, IW could be an activity that is engaged in during both peace and conflict, and that calling a peacetime activity " information warfare" could suggest the applicability of the laws of war (102). The article mainly focuses on IW as using information systems for offensive and defensive purposes in discussing the applicability of the law of armed conflict (LOAC) (102). The author analyzes the three basic principles of LOAC: military necessity, humanity, and chivalry as they might apply in IW scenarios.

He states that the principle of military necessity only allows for the application of that degree of regulated force required for the partial or complete submission of the enemy with least expenditure of life, time, and physical resources (105). He discusses an IW scenario where one would cut or deny all of an enemy's information-transfer media, and states that the "all-inclusive nature" of such an attack raises legal issues including:

1. its scope probably exceeds the bounds of military necessity
2. it probably violates international telecommunications treaties, and
3. it probably violates treaties concerning neutrals (105).

Specifically, he suggests that denying all information-transfer media would disable a country's stock market, banking and air traffic control systems and emergency dispatches, resulting in the loss of civilian lives that is disproportionate to the military objective (105).

Another point he highlights from *Cornerstones of Information Warfare* is the "troubling asymmetry between offensive and defensive actions under information warfare":

> The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of information warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military information functions. There are many information functions critical to our national security that lie outside the military's defensive purview. (Cornerstones)

He states that reliable sources estimate that over 95 percent of military communications traffic travels across commercial communications systems (105). He raises two questions with regard to military necessity and military combatants:

1. If teenage hackers in the enemy's country unilaterally decide to aid their government by creating havoc through their use of computers, are they now fair game for attack by the opposition?

2. If civilian radio and television stations unwittingly broadcast coded messages to the enemy's troops, can they be attacked? (106)

He states that the principle of humanity aims to prohibit the use of force beyond that which is necessary in war to achieve partial or complete submission by the enemy with minimal loss of life, time and resources (106). He points out a problem which arises when identifying some computer programs as "weapons," such as logic bombs or worms, stating that LOAC requires that any nation desiring to implement a new weapon make a determination prior to its use as to whether it complies with the principle of humanity (106).

In discussing the principle of chivalry, the author points out that LOAC prohibits perfidy (treachery) and presents an applicable IW scenario for consideration (108):

> For instance, suppose Iraq sent a bogus E-mail message to low-level coalition force commanders in the Persian Gulf purporting to be from the commander of all coalition forces indicating that Iraq has surrendered and all hostilities are to cease immediately. If a commander acted on this message, believing it to be real and suffered heavy casualties from an Iraqi force he thought was surrendering but was actually attacking, would Iraq be guilty of violating the law of armed conflict? (108)

In discussing the role of neutrals, the author points out that normally, to maintain neutrality, nation-states must not allow aggressors to cross their territory or use their ports for other than emergencies, and asks how the concept applies in the information age where communications channels cross multiple territories (109). Citing Articles 8 and 9 of the Convention on Neutrals, he states that a neutral could allow aggressors to use its communications media without risking neutrality, but that if the neutral were to prohibit use of its communications media to an aggressor, it would have to so unilaterally to maintain neutral status (109). In concluding, the author points out that many of the issues

raised regarding IW are without clear precedent, and that most of the law that legal scholars look to for guidance was developed long before IW concepts were envisioned (109).

Information Warfare: The Next Major Change in Military Strategies and Operational Planning. They author discusses the main objective of conflict between developed nations as being unchanged in the future, including attacks on infrastructure, communications, power, transportation, finance and computational systems that the (adversary's) military and industry rely on (11). He states that when the flow of information is disrupted or loses credibility, the "Information State" becomes paralyzed and cannot act decisively (11). He states that the point of the article is that IW has the potential to by-pass the battlefield and disrupt an enemy's infrastructure essentially stopping a war before it starts (11). He describes IW as a precision blunderbuss that can simultaneously hit more than one element of national power including political, diplomatic, economic, and military (15). He suggests that what is missing in IW is the organizational structure and doctrine required for it to reach its full potential (16). He suggests a "rainbow suit" organizational structure that combines political, diplomatic, economic and military efforts working as an integrated team (coalition) to serve as an effective deterrent force against IW (16). The author states that such a coalition would be difficult to assemble, and that there are technological, cultural, and policy issues to contend with in undertaking such an endeavor (19).

Strategic Information Warfare: A New Face of War reports the results of a study conducted by RAND in support of developing and achieving national IW goals; a

task set out for the IW Executive Board by the Secretary of Defense (82). The study resulted in identifying seven strategic IW features, which are described below:

1. Low entry cost: no requirement for substantial financial resources or state sponsorship,

2. Blurred traditional boundaries: geographic, public versus private interests, and war versus criminal acts,

3. Expanded role for perception management: the power of deception can be increased using image-manipulating and other information-based techniques, thus complicating government efforts to build political support for security-related initiatives,

4. A new strategic intelligence challenge: strategic IW vulnerabilities and targets are not well-understood which impacts classical intelligence collection and analysis methods,

5. Formidable tactical warning and attack assessment problems: lack of an adequate tactical warning system for discerning strategic IW attacks from other activities,

6. Difficulty of building and sustaining coalitions: reliance on coalitions is expected to increase security posture vulnerabilities to strategic IW attacks tipping the scale in favor of opponents,

7. Vulnerability of the U.S. homeland: information-based techniques for strategic IW render geographic al distance irrelevant. (86)

The authors report that the features and consequences of strategic IW lead to the conclusion that key national military strategy assumptions are obsolete and inadequate for confronting the strategic IW threat (90). They give five recommendations as starting points for addressing this problem:

1. Leadership: Who Should Be in Charge in the Government? The Executive Office of the President should be the focal point to ensure that necessary interagency coordination between government organizations involved and Congress is handled effectively. Once this

high-level leadership framework is established, a review of national-level strategic IW issues should be initiated. (90)

2. Risk Assessment. Immediately after establishing the leadership framework described above, conduct a risk assessment to determine the vulnerability of key elements of current national security and national military strategy to strategic IW. (91)

3. Governments Role. Should be part leadership, and part partnership with the domestic sector. The government may play a more productive and efficient role as facilitator and maintainer of some information systems and infrastructure, and through policy mechanisms such as tax breaks, encourage reducing vulnerability and improving recovery and reconstitution capability. (91)

4. National Security Strategy. Needs to address preparedness for the threat as identified, including crossing traditional boundaries such as military to civilian, form foreign to domestic, and from national to local. This may include the concept of having a minimum essential information infrastructure, consisting of information systems, procedures, laws, and tax incentives to ensure the nation's continued functioning in the event of a sophisticated IW attack. (91-92)

5. National Military Strategy. Should account for reduced significance of distance as a player in strategic IW weapons deployment and employment. (92)

The authors conclude by stating that when the President asks whether the U.S. is under IW attack, and if so, by whom, and whether the U.S. military plan and strategy are vulnerable "we don't know" will not be an acceptable answer (92).

Information War and the Air Force: Wave of the Future? Current Fad? offers suggestions on how the Air Force should view and prioritize IW issues in preparing for future operations (1). Areas discussed including how to think and talk about IW, how information can be used to support (air) combat operations, and the role of information in U.S. national security (1-2). In discussing how to think and talk about IW, the author

suggests military commanders approach the issue by seeking answers to the following questions:

1. What information does the U.S. need to conduct any particular operation, and how can that information be obtained?

2. Can the U.S. conduct information-intensive operations in a hostile environment against a competent adversary?

3. Can the U.S. deny the enemy the information necessary to conduct effective operations to meet *its* objectives and to thwart U.S. operations? How? (4)

He states that this approach will yield more direct answers to operational questions, and help integrate the various elements of IW such as computer security, psychological operations, and precision strike with other combat tasks resulting in effective operational plans and more precision in planning (4).

The author states that one of the most important problems the Air Force has to solve is orchestrating the process of getting the right information, putting it into a usable form, and getting it to where it needs to go in a timely manner (4). He states that the Air Force should make its first priority taking advantage of the information revolution to support its combat operations by dealing with the broad spectrum of information operations (4). He warns of the danger of institutionalizing IW with centers of IW and information-focused organizations because they may be counterproductive, and advocates integrating information considerations into all operations and across all organizations (5). He raises the following questions for consideration by planners of future combat operations:

1. What are the payoffs for various levels of adaptive planning in combat operations?

2. How much planning flexibility is technically feasible and affordable?

3. Does the Air Force retain certain current planning vehicles, such as the Air Tasking Order (ATO)? If so, how will it change? If not, what will replace it?

4. How does the military adjudicate the problem of information flow versus chain of command? How does it reconcile "commanders prerogatives" with combat efficiency while avoiding chaos?

5. How far can combinations of various types of sensors on different platforms go in providing a complete, operationally useful, and continuous picture of the battlefield? What is the most cost-effective combination of sensors, platforms, and processing facilities to provide the necessary information?

6. How can the damage assessment problem be solved adequately, particularly when more-sophisticated weapons that rely on relatively subtle damage mechanisms are used?

7. How does the U.S. construct a command, control, communications, computers, and intelligence (C4I) architecture that will satisfy the needs of all the disparate users?

8. What are the impediments to introducing improved technology effectively?

The author states that the U.S. will likely be more critically reliant on information-based systems and strategies, and as such, will be more vulnerable to their disruption than most potential adversaries (6). He states, "vulnerability is the flip side of the leverage that information offers" (6).

In discussing the role of information in U.S. national security, the author states that the Air Force needs to understand the broader (national) problem in formulating its

own IW strategy (13). He poses three basic questions for IW in a national security context: How serious is the problem? What can be done, and how well is it likely to work, and who should, and who can, do it? He states that the National Institute of Standards and Technology (NIST), and the National Computer Security Center (part of the National Security Agency (NSA)) have been given the responsibility of protecting the National Information Infrastructure (NII) as part of the Computer Security Act of 1987 (14). However he also points out that neither of the agencies involved has the budget, power, or expertise to "effect real changes in the manner that computer systems vital to the national interest are protected" (14). He also states that they do not have legal authority over privately owned systems such as the electric power grid and telephone networks (14). He emphasizes the need for a national policy that defines U.S. nation information interests, establishes a priority among computing objectives, and assigns enforcement responsibilities (14). He concludes by recommending that the Air Force's priorities for "waging war in the information age" be:

1. Integrating information systems and concerns effectively into "normal" combat operations,
2. Designing an information architecture and infrastructure that is robust against casual meddling, enemy action, or "bad karma,"
3. Denying enemies the effective use of information using whatever means are most appropriate. (15)

The Advent of Netwar is a documented briefing that provides an overview of the concept called "Netwar" (iii). The Netwar concept was developed to gain an understanding of conflict and crime in the information age (iii). Netwar encompasses

low-intensity conflict (LIC), and operations other than war (OOTW) (3). Netwar involves conflict and crime within society and calls for measures short of war, and involves protagonists who rely on network forms of organization, doctrine, strategy, and communication (5). The protagonists may include terrorists, criminals, fundamentalists, radicals and revolutionaries, and non-violent activists (5).

The authors suggest that Netwar is a natural next mode of conflict and crime as the network form becomes a source of power, and that this power is migrating to those skilled at developing networks (43). They point out that non-state low-intensity adversaries are ahead of governments at using the network form of organization, and that the information revolution is both a force multiplier and force modifier for networks (43). They suggest an interagency approach to combat Netwar that is built across four levels; organizational, doctrinal, technological, and social (85). Organizationally, interagency mechanisms should mix hierarchical and network forms, institute doctrine and operational concepts that match network organization, use technology to develop interagency information and communication systems, and from a social standpoint, train teams to think and behave in network terms (85). The authors suggest that new research centers may be needed to study information (as a concept, academic discipline and military science), organization, doctrine, strategy, and technology to cope with netwar (87). They advocate the establishment of hubs to act as clearinghouses to efficiently coordinate ideas, eliminate duplication, and bridge the networks of academics, soldiers and civilian authorities (87).

Security in Cyberspace: Challenges for Society, Proceedings of an International Conference. RAND and the Ditchley Foundation co-sponsored an international conference in Santa Monica, California on cyberspace security in April 1996, which was attended by Americans, some Canadians, and Europeans described as senior-level intellectual leaders (iii). The major themes that emerged from the conference were:

1. *Cyberspace vulnerabilities are pervasive throughout society*: This is a basic aspect of the cyberspace security problem, given that most of the developed world heavily relies on computer-controlled activities and infrastructures (43),

2. *The number of actors conducting harmful acts in cyberspace is numerous and growing*: The actors range from individuals and small groups to organizations and nation states. They steal information, corrupt data, programs and systems for financial gain, revenge, industrial espionage, or to advance a cause, among other things (43),

3. *Our current understanding of the threats posed by these actors is poor*: There is little quantitative, statistically valid data to describe the problem, and little is being done to collect the needed data. Other problems include fragmented and incomplete understanding of the threat and differences in opinion about the threat (44),

4. *Awareness of cyberspace risks is generally low; complacency is widespread*: Knowledge on the part of the "average user" regarding cyberspace threats is low. Many networked users do not understand the implications of logging-on, transferring and downloading files (44),

5. *There are a number of impediments to improved cyberspace security*: Lack of governmental policy, standards of behavior, clarification of public and private responsibilities, high-quality security software, strong encryption for public use, in addition to widespread societal ignorance of threats and risks (45),

6. *All effective solution strategies should have certain common characteristics*: These include solutions that are driven by the needs of

business, law enforcement and national security, delivered by the private sector (facilitated by an appropriate governmental policy/legal framework, and these solution will require widespread education (46),

7. *There are a number of different dimensions to cyberspace security*: These include economic/legal, military/national security, and social/political (46),

8. *Different security paradigms are appropriate for each of these dimensions*: Economic/legal: use a policing paradigm for effective security structure, military/national security: common defense versus IW should be the paradigm, and social/political: Free speech in cyberspace to promote social harmony and political stability throughout the world (46),

9. *International cooperation is required in every dimension of cyberspace security*: Economic/legal: cooperation on substantive and procedural law, military/national security: sharing information among allies, and social/political: ensure that "free speech in cyberspace" promotes stability versus instability (47),

10. *Today, the "Good Guys" are not winning the battle for security in cyberspace*: The apparent number and magnitude of security incidents is continually rising and involving more bad actors and nations (47),

11. *Disaster may be necessary before adequate security is achieved in cyberspace*: It will take disasters that impact individuals, organizations and the larger society before they become involved in taking responsibility for security (48).

Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach. This document analyzes the development of Air Force IW operational doctrine (4). The author presents a critical analysis of Air Force doctrine documents and discusses steps the Air Force could take in continuing IW doctrine development (4). Citing the 1994 Air Force Issues Book, he points out that the Air Force established IW as a priority in 1993 and was in the process of developing IW policy,

doctrine and a master plan (27). His analysis centers on *Cornerstones of Information Warfare* and draft 1 of Air Force Doctrine Document 5 (AFDD 5), *Information Warfare Doctrine*. AFDD 5 is currently AFDD 2-5, *Information Operations*, and is in its third draft form.

He points out several problems in the language used in *Cornerstones* and AFDD 5 in comparing objectives of air warfare (AW) and IW (32-33). The IW objectives discussed are control, exploit and enhance. With regard to IW control, he points out that in the *Cornerstones* definition, the information realm is controlled so it can be exploited, which is its own objective (32). *Cornerstones* objective: exploit control of information to employ IW against the enemy, in the context of AW, is like saying that an objective of AW is to exploit control of the air to employ AW, according to the author (33). He also states, with regard to the objective of enhance, that both AFDD 5 and *Cornerstones*, erred. In using the phrase "by fully developing military information functions" the drafters overly narrowed the objective such that the Air Force could only enhance overall force effectiveness by fully developing activities involved in the acquisition, transmission, or storage of information (33). The author suggests rewriting these objectives after thoroughly understanding the premise behind the writing of the AW objectives as this would allow for a common ground of thought (33). He offers the following rewrite of AFDD 5 IW objectives:

1. Control: the information realm while protecting our forces from enemy action
2. Exploit: control of the information realm to employ forces against the enemy
3. Enhance: our overall force effectiveness. (34)

The author states that there is also some confusion between AFDD 5 and *Cornerstones* on the definition of Information Operations (IO) (36). AFDD 5 labels IO as "Information Functions", and *Cornerstones* defines IO as "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces" (36).

In looking into the future, the author states that the challenge will be to use Air Force basic doctrine as the foundation to develop IW doctrine for conducting an "Information Campaign" (39).

The Need for a USAF Information Warfare (IW) Strategy For Military Operations Other Than War MOOTW. This document highlights some of the problems that need to be addressed in Air Force IW strategy. The author discusses the importance of Information Infrastructures (IIs) and states that more and more, the U.S. national security posture is dependent upon the National Information Infrastructure (8). He also points out that the IIs are very complex and rely on other infrastructures such as the electrical power grid (8). He states that the IIs currently are very vulnerable to intruders such as foreign intelligence agents, hackers, insiders, drug cartel members, and members of organized crime (8). He states that there are several problems regarding the infrastructure vulnerabilities including lack of a consensus among various agencies and organizations in the U.S. on a national information policy, and no commonly agreed upon terms or definitions for dealing with IW issues (9). Other problems he highlights include varying perceptions on IW issues and matters of jurisdiction nationally or internationally (12).

Information Warfare in a Joint and National Context. The author states that IW may make every area of the U.S. information infrastructure vulnerable to attack in ways never imagined, and that a national debate and IW policy are urgently needed (ii). In discussing joint IW doctrine, he states that it currently is lacking in that it is narrowly focused on command and control warfare (C2W) operations, a subset of IW (4). He states that joint doctrine does not address the global information environment, IW operations in coordination with other government agencies, and lacks standard definitions for IW terms (5). He states that Air Force IW doctrine is contained in *Cornerstones of Information Warfare* and draft 1 of AFDD 5, *Information Warfare*, but that these documents do not address the breadth and scope of future IW operations (6). He states that doctrine needs to comprehensively address how warfighters will deal with adversaries throughout the global information environment, not just within the military information environment or command, control and communications of an adversary (6). He advocates involving the entire nation in examining and discussing the principles of IW and how they can best be employed (12). He states that we need a national policy that addresses all elements of both the national and global information environments, the responsibilities of the DOD and other agencies, and how they will coordinate (25).

Information Warfare and the Lack of a U.S. National Policy. The author states that many agencies and departments in both government and the private sector are independently working the (IW policy) problem (ii). The author suggests that a policy statement from the Executive Branch which places the responsibility on a single agency or committee to integrate the fragmented efforts of government and private industry is the

best approach for achieving a coherent national security program regarding IW (ii). He states that Congress has enacted legislation assigning some responsibilities at a macro level, but the legislation lacks details on specific responsibilities (15). He gives several examples of committees formed by Executive Order (EO) or Presidential Decision Directive (PDD), made up of government and civilian leaders to address national security issues. These include the Security Policy Board established by PDD 29 in 1994, and the National Security Telecommunications Advisory Committee, established by EO 12382 in 1982 (22). He states that committees such as these have the necessary mix of government and private industry leaders to establish a single authority to implement a coherent national policy for security of our national information systems (22).

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. The General Accounting Office (GAO) was tasked by Congress of review and report on DOD computer system attacks, assess the potential for further damage in future attacks, and identify challenges of securing sensitive information (3). They reported that attacks on Defense computer systems are a "serious and growing threat" , and that the exact number of attacks is difficult to determine because only a small amount of attacks are detected and reported (3). Data from the Defense Information Systems Agency (DISA) indicated that the DOD may have experienced 250,000 attacks in 1995, and that attacks are successful 65 percent of the time, and that the number of attacks doubles each year (3). The report concluded that the DOD could take some basic steps to improve its security posture from these intrusions including

strengthening; computer security polices and procedures, security training and staffing, and detection and reaction programs (26).

Assessments Necessary in Coming to Terms with Information Warfare. The author discusses the future of IW and its implications for the military. He states that low cost technology allows anyone to engage in IW including rogue gangs, criminals and curious individuals (48). He makes three key determinations regarding IW:

1. There are no written rules of engagement for IW, anyone can participate and can have access to the technology,
2. The military must bring information into better balance with its arsenal of weapons, and
3. For the near future, the best IW offense is a sound defense. (4)

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Ed. This report discusses and summarizes the breadth and complexity of policy and strategy issues (P-1). It states that the nature of IW complicates information protection and assurance (1-4). Several aspects of the nature of IW given in the report include:

1. anonymous adversaries and many targets
2. simple technology
3. ambiguous law; criminal act versus act of war
4. no spatial, geographic, temporal or political boundaries. (1-5)

The report also discusses the nature and complexity of information infrastructures (IIs) and states that there is no simply way to define, establish bounds for, measure impact of, or identify evolutionary responsibilities for operation, maintenance and repair

of IIs (2-15). The report lists the elements of IIs in a series of five tables. Table 6. Information Infrastructure Elements was developed mainly from the five tables.

Table 6. Information Infrastructure Elements

Components	Networks and Services	Domains	Stakeholders	Stakeholder Interests
Computers/ Printers	Public Switched Telephone Network	Health and Safety	Federal Government	Information Assurance
Telephones	Internet	News	Military	Jobs
Cable/Wire/ Optical Fiber	Direct Broadcast Satellite (TV)	Law Enforcement	Economic Marketplace	National Security
Satellites	Encryption	Navigation	Industries	Regulation
Cameras	Cable TV	Government	Congress	Interoperability
Switches	On-line Services	Military	Academia	Technologies
Television	Power Networks	Intelligence	Citizens	Interconnection
Fax Machines	Cellular Networks	Weather	State Governments	Standards and Protocols
Microwave Nets	Transportation Networks	Transportation	Labor Organizations	User-friendly Interfaces
Compact Disks	Commercial Satellite Networks	Entertainment	Public Servants	Privacy (Security)
Video/Audio Tape	Financial Networks and Services	Education	Political Groups	Intellectual Property Rights

(Adapted from SAIC, pp. 2-16, 2-17, Tables 2-1-3, 2-1-4, 2-1-5, 2-1-6, and 2-1-7)

The Findings and Observations section of the report highlights the following problems that need to be resolved:

1. Within the Federal government and the private sector, there is no set of universally agreed-upon terms and definitions for discussing IW and information assurance issues in a common framework (3-3),

2. There is a lack of understanding of the dependency on and influence of vulnerable infrastructures (3-4),

3. The perceptions of IW issues are based on individual experiences and organizational missions and functions (3-5),

4. Responsibilities for information protection are not consistently assigned within the Executive Branch departments (3-5),

5. With the exception of the telecommunications infrastructure, there are no organizational structures and processes to facilitate the sharing of sensitive information (threat and vulnerability information) needed for infrastructure assurance (3-6),

6. Very few organizations have developed a capability to identify the nature of disruptions or intrusions (assuming they are detected), to restore the infrastructure in the event of intrusions, or to adequately respond to IW attacks (3-6),

7. In many organizations, budgets and staff to address information assurance issues are too small to address information assurance needs (3-6),

8. All organizations are constantly changing making information assurance a subordinate concern to operational and fiscal crises. (3-7)

The report also indicates that progress in being made in the following areas:

1. Executive-level understanding of IW issues is increasing through press and trade publication coverage, and through information security demonstrations for senior executives in some departments (3-7),

2. Individual and collective agency coordination efforts are becoming more focused (3-7),

3. Information infrastructure protection is gaining Congressional support through legislation (3-7),

4. Press and trade coverage is increasing visibility of information infrastructure assurances issues (3-7),

5. Policy discussions are leading to IW-related directives and guidance such as CJCSI 6510.01A, *Defensive Information Warfare*, CJCSI 3210.01, *Joint Information Warfare Policy*, and the OMB's Revised Appendix III to Circular A-130 (3-8),

6. Military service efforts have made contributions to increase understanding of issues and coordination of effort including the establishment of operational IW organizations (3-8),

7. Defense-wide efforts on IW issues include departmental IW training activities, research efforts to support information assurance, efforts to integrate information operations courses into the course curriculum at the National Defense University colleges (3-8),

8. Federal departments and agencies are coordinating activities such as the computer crime issues group formed by the FBI and U.S. Secret Service (3-9),

9. The creation of computer emergency and incident response capabilities is increasing in the DOD, civil agencies and private sector. (3-9)

From Hackers to Projectors of Power, Information Warfare. The author singles-out 1993 as the year in which awareness over IW concerns became focused citing the creation and publishing of several documents including:

1. War and Anti-war: Survival at the Dawn of the Twenty-first Century, by Heidi and Alvin Toffler,

2. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War, By Al Campen,

3. CJCS Memorandum of Policy (MOP) 30, Command and Control Warfare

4. DOD Directive TS-3600.1, Information Warfare, (top secret). (6)

He also discusses the nature of information and offers the following for consideration with regard to its potential impact on states, military institutions, individuals and society:

1. the value of information is infinite and thus, incalculable,

2. one can give information away and still possess it,
3. one can have information stolen and not know it,
4. one can observe the theft of information and have no idea who or where the perpetrator is,
5. information knows no geographical boundaries, and
6. information recognizes no sovereignty. (7)

Report of the Defense Science Board Task Force on Information Warfare.

The Defense Science Board Task Force on IW was asked to:

1. Identify the users of national interest who can be attacked through the shared elements of the NII,

2. Determine the scope of national information interests to be defended by IW defense and deterrence capabilities,

3. Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the NII and the information users of national interest,

4. Identify the indications and warning, tactical warning and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the NII and/or attacks on information users of national interest,

5. Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national IW-defense capability, and

6. Provide specific guidelines for implementation of their recommendations. (3)

The report identifies the users of national interest who can be attacked through the shared elements of the NII, as:

> those who are responsible for performing the critical functions necessary for the delivery of goods and services upon which our political, military, and economic interests depend. (8)

The scope of national information interests to be defended by IW defense and deterrence capabilities include critical functions that have national security implications and the supportive infrastructure systems and information needed for their performance (8). The report lists the national interests that must be defended, under the national goals for IW defense as;

1. strategic nuclear deterrence,
2. continuity of government,
3. IW indications and warning, minimum essential information infrastructure to manage restoration of critical functions such as emergency response,
4. minimum information and systems required to deploy quick reaction conventional forces, and
5. other critical DOD and national (civil) functions and infrastructures based on importance and available resources such as DOD operations and deployment, banking and commerce, and electrical power and telecommunications. (41)

The concept for developing procedures, processes, and mechanisms required to defend against various classes of threats to the NII and the information users of national interest includes deterrence as a first line of defense (9).

The report also states that it is technically and economically impossible to design and protect the infrastructure to withstand any and all disruptions and attacks, or to avoid all risk (9). It states that risk can be managed by protecting selected portions of the infrastructure that support critical functions and activities for maintaining political,

military, and economic interests (9). The report suggests the following principles be applied in the defense concept:

1. Critical functions must be capable of being performed in the presence of IW attacks,
2. Some minimum essential infrastructure capability must exist to support these critical functions,
3. Point and layered defenses are preferable to area defenses,
4. The infrastructure must be designed to function in the presence of failed components, systems, and networks and address risk management issues,
5. The infrastructure control functions should not be dependent on normal operation of the infrastructure, and
6. The infrastructure must be capable of being repaired. (9)

The efforts of the Task Force resulted in the formation of 13 recommendations that they consider as imperatives (9). Each of these recommendations is briefly presented in the following paragraphs.

1. *Designate an accountable IW focal point.*

The Task Force identified this as the most important recommendation (10). The Task Force stated that the Secretary of Defense needs a single focal point charged to provide staff supervision of the complex activities and interrelationships that are involved in IW including oversight of both offensive and defensive information warfare planning, technology development and resources (10). The report outlined specifically what the SECDEF should do:

1a. Designate ASD(C3I) as the accountable focal point for all IW issues.

1a(1). Develop a plan and associated budget beginning in FY 97 to obtain the needed IW-D capability.

1a(2). Authorize ASD(C3I) to issue IW instructions.

1a(3). Consider establishing a USD(Information).

1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible (10).

2. *Organize for IW-D.*

This Task Force recommendation identifies the need for specific IW-D related capabilities and organizations to provide or support them (11). It calls for:

2a. establishing a center to provide strategic indications and warning, current intelligence, and threat assessments

2b. establishing a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities.

2c. establishing an IW-D planning and coordination center reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations center to develop an IW planning framework; assess IW policy, plans, intelligence support, allocation of resources, and IW incidents; develop procedures and metrics for assessing infrastructure and information dependencies; and facilitate sharing of sensitive information such as threats, vulnerabilities, fixes, tools, and techniques within DOD and among government agencies, the private sector, and professional associations. (11)

2d. establishing a joint office for system, network and infrastructure design to develop and promulgate IW-D policies, architectures, and standards; design the information infrastructure for utility, resiliency, and security; develop and implement an IW-D configuration management

process; and conduct independent verification of design and procurement specifications to ensure compliance with the design. (12)

2e. establishing a Red Team to independently assess the vulnerabilities of new systems and services and conduct "IW-like" attacks to verify the readiness posture and preparedness of the fighting forces and supporting activities. (12)

3. *Increase awareness.*

The Task Force suggested making senior-level government and industry leaders aware of the vulnerabilities and of the implications including:

3a. establishing internal and external IW-D awareness campaigns for the public, industry, CINCs, Services, and Agencies,

3b. expanding the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII,

3c. reviewing joint doctrine for needed IW-D emphasis,

3d. exploring the possibility of large-scale IW-D demonstrations in order to understand the cascading effects and collecting data for simulations,

3e. developing and implementing simulations to demonstrate and play IW-D effects (USD(A&T) lead),

3f. implementing policy to include IW-D realism in exercises, and

3g. conduct IW-D experiments. (12)

4. *Assess infrastructure dependencies and vulnerabilities.* To include:

4a. developing a process and metrics for assessing infrastructure dependency,

4b. assessing/documenting operations plans infrastructure dependencies,

4c. assessing/documenting functional infrastructure dependencies,

4d. assessing infrastructure vulnerabilities,

4e. developing a list of essential infrastructure protection needs,

4f. developing and reporting to the SECDEF the resource estimates for essential infrastructure protection, and

4g. reviewing vulnerabilities of hardware and software embedded in weapons systems (13).

5. *Define threat conditions and responses.* Including:

5a. defining and promulgating a useful set of IW-D threat conditions which is coordinated with current intelligence community threat condition definitions,

5b. defining and implementing responses to IW-D threat conditions, and

5c. exploring legislative and regulatory implications. (13)

6. *Assess IW-D readiness.* Including:

6a. establishing a standardized IW-D assessment system for use by CINCs, Military Departments, Services, and Combat Support Agencies, and

6b. incorporating IW preparedness assessments in Joint Reporting System and Joint Doctrine. (13)

7. *"Raise the bar" with high-payoff, low-cost items.* Including:

7a. directing the immediate use of approved products for access control as an interim until a MISSI solution is implemented and for those users not programmed to receive MISSI products,

7b. examining the feasibility of using approved products for identification and authentication, and

7c. requiring the use of escrowed encryption for critical assets such as databases, program libraries, applications, and transaction logs to preclude rogue employees from locking up systems and networks. (13)

8. *Establish and maintain a minimum essential information infrastructure.*

Including:

8a. defining options with associated costs and schedules,

8b. identify minimum essential conventional force structure and supporting information infrastructure needs,

8c. prioritizing critical functions and infrastructure dependencies,

8d. designing a Defense MEII and a fail-safe restoration capability, and

8e. issuing direction to the Defense Components to fence funds for a Defense MEII and fail-safe restoration capability. (14)

9. *Focus the R&D.* Including:

9a. developing robust survivable system architectures,

9b. developing techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems,

9c. developing tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks,

9d. developing tools for synthesizing and projecting the anticipated performance of survivable distributed systems,

9e. developing tools and environments for IW-D oriented operational training,

9f. developing test-beds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics,

Also, the SECDEF should work with the National Science Foundation to:

9g. develop research in U.S. computer science and computer engineering programs, and

9h. develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices. (14)

10. *Staff for success.* To include:

10a. establishing a career path and mandate training and certification of systems and network administrators,

10b. establishing a military skill specialty for IW-D, and

10c. developing specific IW awareness courses with strong focus on operational preparedness in DOD's professional schools. (14)

11. *Resolve the legal issues.* Including:

11a. promulgating for DOD systems:

- guidance and unequivocal authority for Department users to monitor, record data, and repel intruders in computer systems for self protection,

- direction to use banners that make it clear the Department's presumption that intruders have hostile intent and warn that the Department will take the appropriate response,

- IW-D rules of engagement for self-protection (including active response) and civil infrastructure support, and

11b. providing to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems. (15)

12. *Participate fully in critical infrastructure protection.* Including:

12a. offering specific Department capabilities to the President's Commission,

12b. advocating the Department's interests to the President's Commission,

12c. requesting the Commission provide certain national-level capabilities for the Department, and

12d. suggesting IW-D roles for government and the private sector. (15)

13. *Provide the resources.* The Task Force's cost estimate for implementing the key recommendations was $3.01 billion over fiscal years 1997 through 2001. However, the Task Force recommended that the Department make a detailed estimate. (15)

Summary of Key IO and IW Doctrine and Policy Issues

Each of the two categories of documentation presented a variety of key issues. They have been combined into a summary in the paragraphs that follow.

The first issue centers on the realization that IW remains vague. The framing of concepts and terminology are still open to debate, and not all of the definitions convey the same message, such as the JCS definition of IW versus the Air Force or Army interpretations. However, conducting a chronological review of documentation revealed that many issues are coming into focus, and news ones are continuously being fleshed-out, such as interagency involvement, public and civil affairs roles, and legal issues.

Although they do not have complete or universally accepted definitions, the boundless information environments and infrastructures have been recognized. The GII, NII, DII, and so on, provide a framework for understanding and considering vulnerabilities, threats, targets, legal and regulatory concerns, responsibilities, international concerns, and most importantly, the need for action in order to protect our national security interests, and preserve our way of life.

The criticality of having solid doctrine as a base for strategic planning on a Joint and National level, as well as within the services, and government departments and agencies is being realized. Several of the documents considered the direction IO and IW doctrine need to be moving in and offered guidance and recommendations, such as *Information Warfare, A Strategy for Peace, The Decisive Edge in War*, *Information Warfare* by George Stein, and *Information Warfare: The Next Major Change in Military Strategies and Operational Planning*. Others posed questions for strategic planners to consider regarding the operationalization of IO such as *Strategic Information Warfare: A New Face of War*, *Information Warfare and the Air Force: Wave of the Future? Current Fad?*, and the *Report of the Defense Science Board Task Force on Information Warfare*.

Integration in training, resource use, education, exercises and operations, and the forming of strategic partnerships, appear to be mandates.

Consider the principles of war in applying information warfare. Consider information operations in the context of social, economic, and political and military decision-making processes. To achieve and maintain information superiority, our information operations doctrine, policy, strategic planning initiatives, missions, goals and

objectives must be properly aligned with our national security objectives. That is the message being sent through the raising of these issues.

Chapter III discusses the research methodology used in this exploratory study.

III. Methodology

Focus of the Study

This study focused on determining whether current and pending unclassified Air Force IO and IW doctrine and policy appears to be progressing in the direction that our national political and military leaders intend it to. This was accomplished through an exploratory study using secondary data, and criterion-based congruence analysis, which will be explained later in this chapter.

The first step was to identify specific investigative questions to establish a framework for the analysis. The investigative questions evolved as a result of several conversations and electronic mail correspondences with the thesis sponsor to identify the specific research problem and answers sought. The investigative questions that were used are listed below:

1. Does Air Force IO and IW doctrine and policy flow naturally and consistently from guidance developed at higher levels?
2. Is Air Force IO and IW doctrine and policy complete?
3. Does Air Force IO and IW doctrine and policy address everyone it needs to at all appropriate levels?
4. Is Air Force IO and IW doctrine and policy consistent with our national strategic objectives and national security?

The next step was to find an appropriate means of analysis. An exploratory study was selected for three reasons. First, the investigative questions that were developed, and answers sought, are qualitative in nature. Although both qualitative and quantitative

techniques can be used in exploratory studies, exploration tends to rely more on qualitative techniques (Cooper and Emory, 118). Second, the definitions and terminology used to describe IW lack clarity and universal consensus. Although some of the underlying themes of IO and IW have been employed for many years, the information age and global electronic connectivity have changed the nature of IO and IW leaving many unresolved issues. Exploratory studies are appropriate when researchers do not have a clear idea of the problems they will encounter during the study (Cooper and Emory, 117). Finally, the breadth and depth of the subject remain largely undefined and without a formal research base. Exploratory studies are used to develop concepts more clearly, establish priorities, and to improve future research design (Cooper and Emory, 118). Thus, an exploratory study was a logical choice for this thesis.

Two approaches that are adaptable for exploratory investigations are document analysis (to evaluate historical or contemporary confidential or public records, reports, government documents, and opinions), and elite interviewing (for information from influential or well-informed people in an organization or community) (Cooper and Emory, 118-119). Both of these approaches were applied in this study. Criterion-based congruence analysis was used for document analysis, and the Delphi technique was used for elite interviewing.

Document Analysis: Criterion-based Congruence Analysis

The first step in document analysis consisted of identifying appropriate secondary data sources for addressing the specific investigative questions. A document search was

conducted that included subject searches at the AFIT Library, World Wide Web topic searches, and document bibliography reviews to trace document origins. These searches resulted in identifying 46 documents relating to IW doctrine and policy. The 46 documents were selected based on their relevance to doctrine and policy formation in general, specific IO/IW doctrine and policy formation, and IO/IW issues germane to doctrine and policy development, such as legal, regulatory, strategic planning, and, roles and missions. The 46 documents were categorized as either Hierarchical literature or Academic literature.

For purposes of this study, Hierarchical literature was defined as coming from an authoritative source within the military chain of command. Hierarchical authorities include the President, Secretaries of Defense and the Air Force, Chairman of the Joint Chiefs of Staff, the Air Force Chief of Staff, and subordinate units within the DOD and Air Force. The Hierarchical literature consisted of 27 policy and regulatory documents ranging from an Executive Order to an Army field manual.

Academic literature was defined as coming from academia, both public and private, or as the result of an authoritatively sanctioned investigation or study. The Academic literature consisted of 19 documents that included research and commentary on IO/IW issues, and doctrine and policy issues.

The next step in document analysis was to select the appropriate means for analyzing the data within each document. This effort, described below, resulted in selecting criterion-based congruence analysis.

Data analysis can be defined as consisting of three concurrent flows of activity; data reduction, data display, and conclusion drawing/verification (Miles and Huberman, 10). Each of these activities, as conducted by Miles and Huberman, is briefly outlined below:

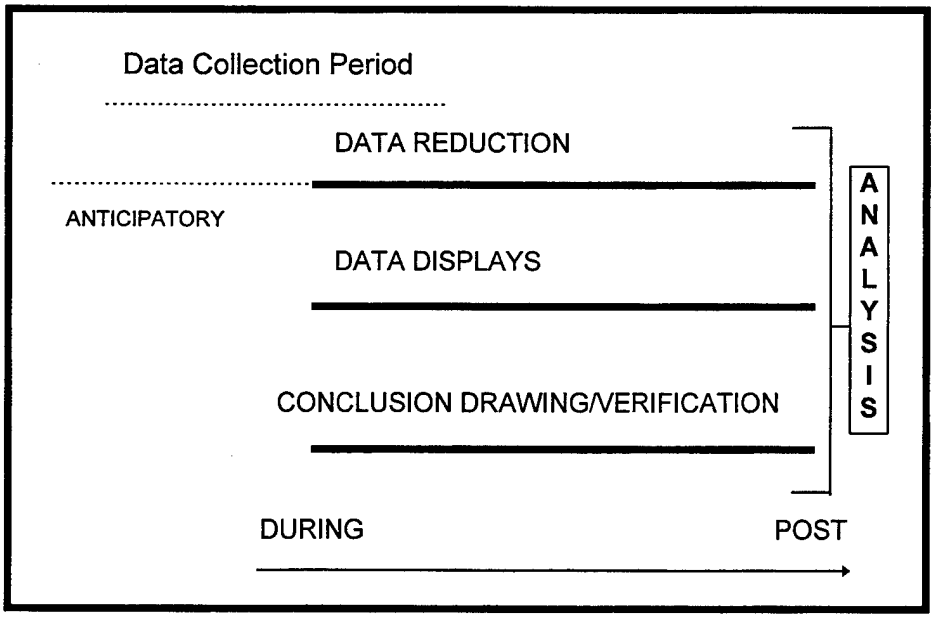
1. *Data Reduction* is the process of selecting, focusing, simplifying, abstracting and transforming data from notes or transcriptions. It is a continuous and iterative process that begins with anticipatory data reduction (Miles and Huberman, 10),

2. *Data Display*, such as in the form of expanded text, graphs, charts or networks, is an organized, compressed assembly of information that permits conclusion drawing and action (Miles and Huberman, 11),

3. *Conclusion Drawing and Verification* consists of determining what things mean, such as noting regularities, patterns, explanations, possible configurations, and propositions. The conclusions are verified as the analyst proceeds, and may be brief, such as in a second thought in the analyst's mind checked against field notes, or by more elaborate means (Miles and Huberman, 11).

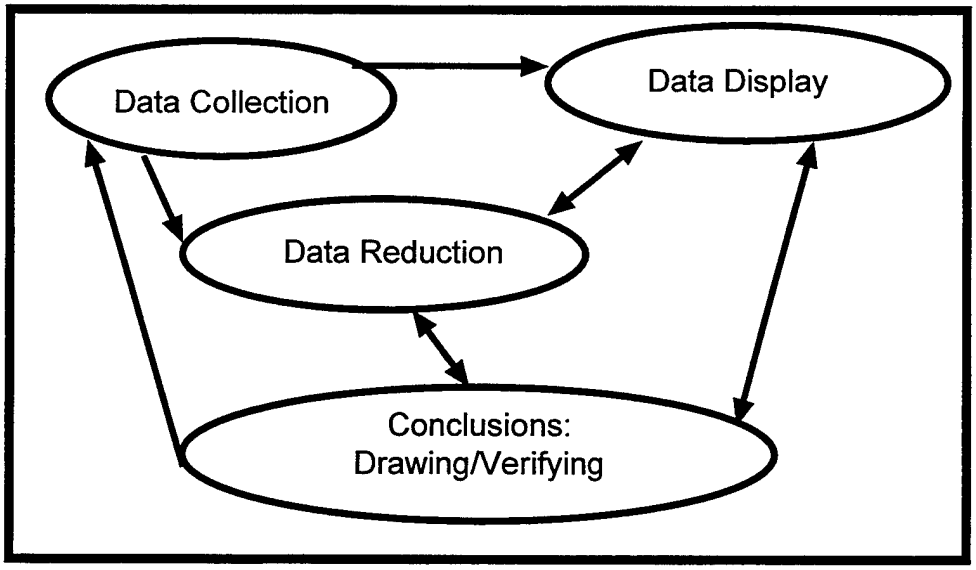
These activities constitute an iterative analysis process that begins with data collection, continues through data reduction, data displays, and the drawing of conclusions and recommendations. The process allows for the data analyst's preconceptions, or anticipatory thoughts, to be included in the analysis.

Miles and Huberman show how these concurrent flows of activity relate to data collection and the overall process of data analysis in two figures. Figure 13 depicts the components of data analysis as they occur over time, or flow through the data analysis process. Figure 14 depicts the relationships of the components of data analysis and their interactions.



(Adapted from Miles and Huberman, page10, Figure 1.3, Components of Data Analysis: Flow Model)

Figure 13. Data Analysis Flow Model



(Adapted from Miles and Huberman, page12, Figure 1.4, Components of Data Analysis: Interactive Model)

Figure 14. Data Analysis Interaction Model

The concepts described by Cooper and Emory, and Miles and Huberman can be combined with use of a Delphi to form a criterion-based congruence analysis model. This model is depicted in Figure 15. Criterion-based Congruence Analysis Model.

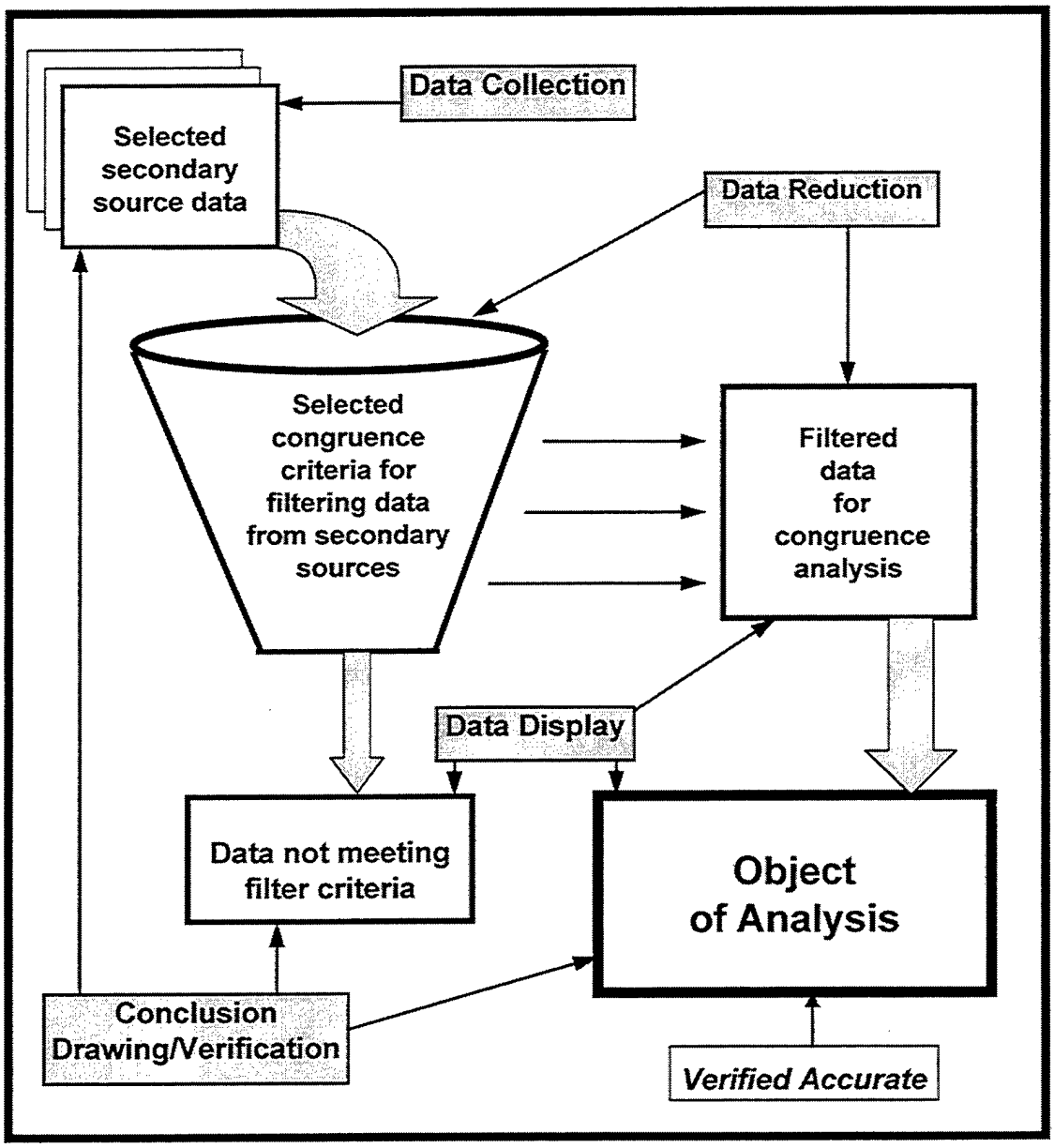


Figure 15. Criterion-based Congruence Analysis Model

The Criterion-based Congruence Analysis Model depicts the data analysis methodology used in this study. The process begins with data collection where documents are selected based on their anticipated value to the study. During data reduction, issues that are believed to be important to the study are selected, focused-on, and simplified for display and for drawing and verifying conclusions. The process is iterative and involves both induction and deduction on the part of the researcher, or what John Dewey referred to as *the double movement of reflective thought* (Cooper and Emory, 28). It allows the researcher to take inputs, in the form of secondary data sources, filter them based on a predetermined set of criteria, and then coalesce or distill the data into conclusions in a simple form. The conclusions can be compared to what was first anticipated during data collection, or recycled through the process, or directly compared to a predetermined object of analysis, which has been verified as accurate by some means appropriate for the study. The entire process can be replicated with ease. The selected congruence criteria for filtering data from secondary sources are described next. Congruence is the quality or state of agreeing, coinciding, or being congruent (Merriam-Webster). Criterion-based congruence then, is the state of agreement based on some specified elements, qualities or characteristics. The qualities chosen to be the criteria for this analysis were *complete*, *consistent*, and *cohesive*. They were chosen because of the assumption that they are desired qualities in doctrine and policy. It is assumed desirable that Air Force IO and IW doctrine and policy be complete in the sense that it addresses all relevant topical issues, that it be consistent with the doctrine and policy created at higher levels in support of our national security interests, and that it be cohesive in the logical

arrangement and presentation of ideas and issues. This would include moving from general to specific IO and IW issues and concepts and addressing them with a similar breadth and depth of discussion as parent doctrine and policy do. This assumption comes directly from the investigative questions (and answers sought), and is a function of addressing the original research problem.

Each of the three criteria is defined below as it was applied to this study.

1. **Complete**: addressing all significant issues, concepts, and requirements directed by authority, as well as those germane to what is known about IO and IW,

2. **Consistent**: applying the same definitions, terminology, and concepts as governing doctrine,

3. **Cohesive**: principles, issues and concepts presented must be integrated internally and flow naturally from those addressed by relevant authority externally.

Figure 15. Criterion-based Congruence Analysis Model, depicts a general model. In this study, the secondary source data consisted of the 27 Hierarchical, and 19 Academic documents that were described above and reviewed in Chapter II. The congruence criteria for filtering data from secondary sources were described above as complete, consistent, and cohesive. The object of analysis that was used consisted of two documents that together encompass current and pending unclassified Air Force IO and IW doctrine and policy; *Cornerstones of Information Warfare*, and *AFDD 2-5, Information Operations*. The application of these specific elements to the Criterion-based Congruence Analysis Model yields Figure 16. Criterion-based Congruence

Analysis Model of Current and Pending Unclassified Air Force IO and IW Doctrine and Policy.

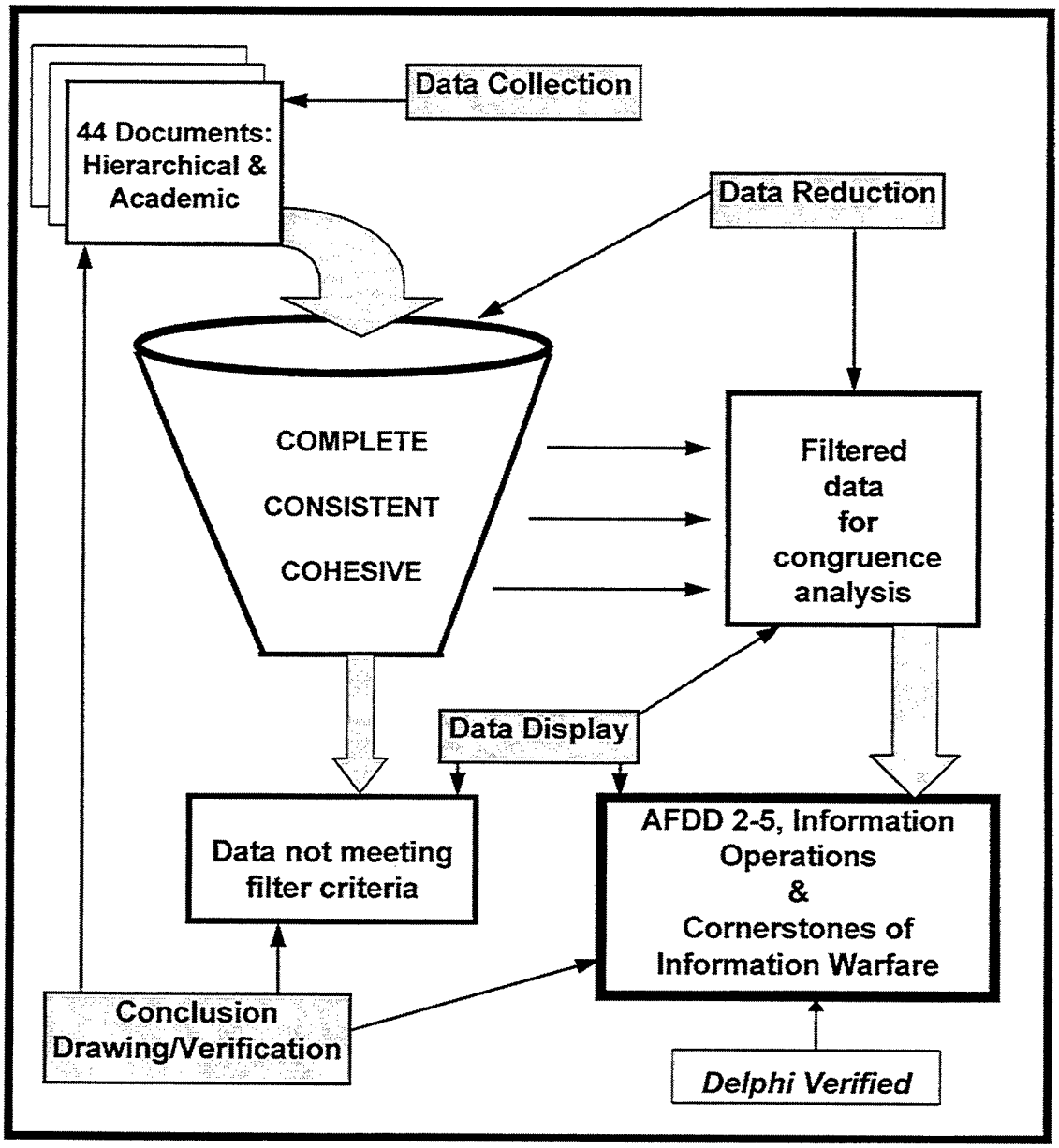


Figure 16. Criterion-based Congruence Analysis Model of Current and Pending Unclassified Air Force IO and IW Doctrine and Policy

Referring to Figure 16, the object of analysis for this study was the model of current and pending unclassified Air Force IO and IW doctrine and policy. How this model was developed and refined for accuracy are described next.

Delphi Technique: Developing the Air Force IO/IW Doctrine and Policy Model

The Delphi technique offers both anonymity, to reduce the possible effect of dominant or influential opinions, and controlled feedback (Dalkey, 3). The Delphi technique is used for eliciting and refining the opinions of a group of people (Dalkey, 1). Normally Delphi group participants are selected based on their expertise in a given area. For this study, the group was selected from individuals who develop, review, advise on, and analyze Air Force doctrine and policy. The Delphi technique was chosen as a means of elite interviewing in this study.

The process of conducting the Delphi involved determining who would be appropriate for Delphi group participation, and then conducting the Delphi rounds and analyzing the results. The group members selected were asked to evaluate the accuracy of a model of unclassified current and pending Air Force IO/IW doctrine and policy.

They were also asked to review a list of 46 secondary source documents to determine if any additional documents should be considered in the analysis. The list of secondary source documents the Delphi group was asked to review is presented in Appendix D: A Suggested Chronology of Key IO/IW Doctrine and Policy Guidance.

Prior to being sent to the Delphi group, the complete set of materials was pre-tested (sent via electronic mail) to five graduate students at the Air Force Institute of

Technology (AFIT). The purpose of the pretest was to determine the clarity of the instructions. Refinements were then made to the complete set of materials prior to sending them out to the Delphi group participants.

Group Selection. For this study, the subjects were selected from individuals who are directly involved with Air Force doctrine and policy, through the development process, review, analysis, or fielding. Additional selection criteria included having knowledge and/or experience working with IO/IW issues with regard to doctrine and policy.

During the data collection period, potential subjects were identified incidentally through unrelated data collection interviews, briefings, and field analysis conducted at the Air Force Information Warfare Center (AFIWC) at Kelly Air Force Base, San Antonio, Texas, through document analysis tracing reference materials and identifying authors, and through unrelated phone conversations conducted for the purpose of obtaining secondary data sources for analysis.

It is important to mention the relationship between the subjects and the doctrine processes described in Chapter II. Figure 2 and Figure 4 depict models of the doctrine development processes at the Air Force and Joint levels. The six subjects who were asked to participate in this research all have direct roles in executing these processes.

These six subjects represent the Air Force Communications Agency, the Air Force Doctrine Center, the College of Aerospace Doctrine Research and Education at Air University, the Operations (J-3) Staff at the Pentagon, the Institute for National Strategic

Studies at the National Defense University, and the Air and Space Operations Staff (Intelligence, Offensive Information Operations) at Headquarters Air Force.

The Model. The model that was used in the first round is presented in Appendix C and Figure 17. Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy. It was developed by examining available Air Force documents that discuss IO and IW doctrine, policy, concepts and strategy, and then selecting those that best exemplified doctrine and policy by content and description.

Figure 17 depicts the two documents that embody current and pending unclassified Air Force IO and IW doctrine and policy. Both of these documents were reviewed in Chapter II. *Cornerstones of Information Warfare,* an Air Force white paper, was developed in 1995, and was the Air Force's first unclassified document that directly addressed IW doctrine and policy issues. At the unclassified level, it represents the origin of IW doctrine and policy for the Air Force. The model depicts this document as a foundation. *AFDD 2-5, Information Operations*, represents a change in thinking with regard to IW doctrine and policy and its evolving concepts. IW has become a subset of Information Operations. The model depicts this document as grounded in, but a clear departure from *Cornerstones of Information Warfare*. Still in draft form, its release is pending approval.

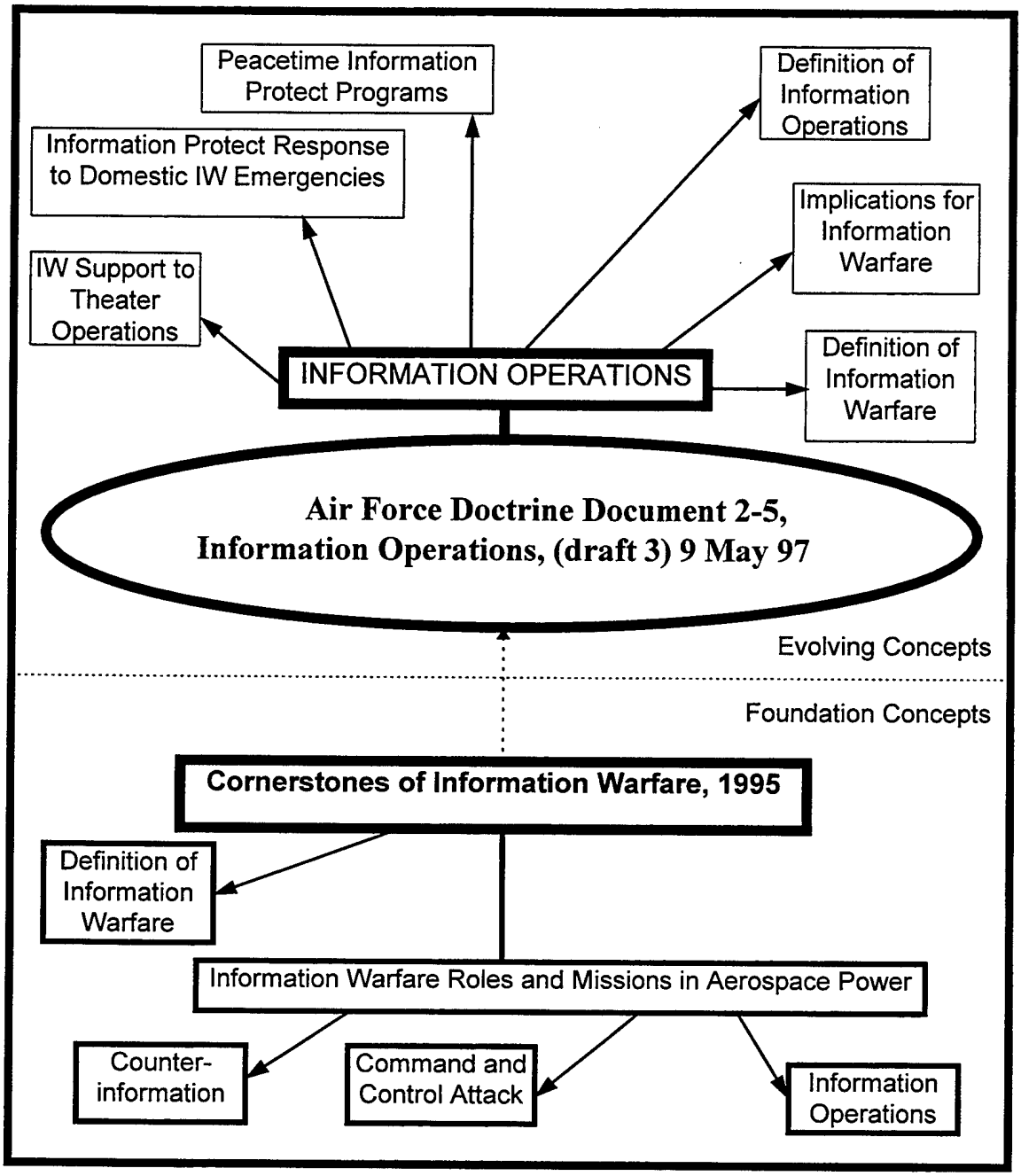


Figure 17. Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy

The Delphi was conducted in 2 rounds. Each round consisted of the Delphi group receiving and responding on the materials they were sent. Between the rounds the materials were modified to incorporate the Delphi responses. The Delphi was concluded after the second round because the group was able to verify that the model was accurate and appropriate for the study. The results of the Delphi rounds are reported in Chapter IV.

Research Assumptions

There are two basic assumptions underlying this research:

1. Enough is known about IO and IW to determine whether Air Force doctrine and policy is complete.
2. Those selected to participate in the Delphi group are appropriate in terms of their experience with doctrine and policy formation, and IO/IW background.

Summary

The methodology applied to this study included the use of the Delphi technique to obtain an accurate model as the basis of analysis and to check for possible relevant secondary source documents that were inadvertently missed.

Qualitative data analysis was conducted through criterion-based congruence analysis which is grounded in Miles and Huberman's concurrent flows of activity. The objective in doing this was to achieve a qualitative measure of congruence between what is known and has been mandated about IO and IW, and the direction the Air Force is

moving in (in terms of unclassified doctrine and policy). Chapter IV presents the results of the Delphi and the criterion-based congruence analysis.

IV. Results of Analysis

The Results of the Delphi Rounds

Round 1. Each of the six Delphi group members received via electronic mail, a cover letter with a brief explanation of the request being made (see Appendix B: Round 1 Delphi electronic mail cover letter), an attachment document containing the model of unclassified Air Force IO/IW doctrine and policy (see Appendix C: Original Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy), and an attachment document containing the secondary source document list (see Appendix D: A Suggested Chronology of Key IO/IW Doctrine and Policy Guidance). They were allotted one week to review the materials and return their comments for this round.

Comments were received from all six Delphi group members and reviewed to determine if the model needed to be refined and to determine if the document list was complete. A comment was received stating that classified documents should be included in the research to make it complete, however, the scope of this research did not allow for review of classified material.

The significant comments received on the model and source document listing from the six Delphi group members are summarized below.

Comments on Model:

1. The model covers the important aspects for IW doctrine and policy.
2. Clarify that now IW is a subset of IO.
3. AFDD 2-5, Information Operations, draft 4, 22 July 97 is available.
4. Include Information Superiority on the evolution side of the model .
5. The model needs supporting documentation for a reader to determine what subordinate considerations are encapsulated within categorical headings of the model.

Comments on Document list:

1. The document list covers the important aspects for IW doctrine and policy.
2. AFDD 2-5, Information Operations, draft 4, 22 July 97 is available.

Comments on the model indicated that significant improvements could be made, and that a second Delphi round was appropriate. Comments regarding the secondary source document list indicated there were no significant additions needed other than a review of the most current version (draft 4 dated 22 July 1997), of *AFDD 2-5, Information Operations*.

The model was amended to include the significant comments. The refined model is presented in Appendix F: Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy.

Round 2. There were no changes in the Delphi group membership for Round 2. Each of the six participants received via electronic mail, a cover letter with a brief explanation of the request being made (see Appendix E: Round 2 Delphi electronic mail cover letter), and an attachment document containing the improved model of unclassified Air Force IW doctrine and policy (see Appendix F: Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy). The group was given one week to review the refined model and comment on its accuracy.

The secondary source document list was not required for the second round. Thus, the comments received from the second round were on the refined model only. The comments received from the second Delphi round are summarized below.

Comments on Model:

1. There are amended versions of draft 4 to AFDD 2-5, *Information Operations* circulating between members in the doctrine development process indicating that there are forthcoming changes to the document that may include changing "counterinformation operations" to "information warfare", and changing "supporting functions" to "information in warfare." Other considerations include the addition of Public Affairs, and removal of "Space Support" as a major supportive function.
2. The model will continue to evolve.
3. Great job on the revised model.
4. The model captures all the important elements of the underlying documents.
5. The model must be held constant for the analysis.

The comments suggested that no significant improvements were needed on the model, and that a third Delphi round was not necessary. Comments 1 and 2 above are significant, however they pertain to an evolving model, rather than one that is fixed in time so that it can be analyzed. Comment 5 concurs with this argument.

Although the processes of developing doctrine and policy are dynamic and their draft products are constantly being revised, for purposes of this research it was decided that the object of analysis should be a fixed model in order to facilitate the analysis. As such, the Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy was used as the object of analysis in the criterion-based congruence analysis. This model appears in Appendix F.

For the remainder of this document, references to the model are made with regard to its underlying documents; *Cornerstones of Information Warfare*, and AFDD 2-5, *Information Operations* draft 4, dated 22 July 1997.

The Results of the Criterion-based Congruence Analysis

The results of the criterion-based congruence analysis are in essence the combined results of the iterative processes of filtering 44 hierarchical and academic documents for data reduction in terms of completeness, consistency, and cohesiveness, and then using the data reduction to analyze, make observations about, and draw conclusions about the object of analysis and its underlying documents (see Appendix F).

The following paragraphs discuss the results of these processes in terms of the Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy being complete, consistent, and cohesive. Where the model appeared to be congruent (complete, consistent, and cohesive), is reported in general terms. Where the model appeared to be incongruent is reported in specific terms.

Complete. For the model to be complete it must address all significant issues, concepts, and requirements directed by authority, as well as those germane to what is known about IO and IW from hierarchical and academic sources.

The model addresses general concepts such as offensive and defensive counterinformation operations, supporting functions of information operations such as intelligence, and theater operations such as planning and organization. These concepts

have been carried forward from many of the hierarchical documents including *A National Strategy of Engagement and Enlargement, Joint Vision 2010, Information Warfare; A Strategy for Peace, The Decisive Edge in War, JP 3-13 Joint Doctrine for Information Operations,* and from *Information Warfare: An Opportunity for Modern Warfare*. The model is incomplete in the following areas:

1. The model does not address deconfliction of responsibilities and application of resources in counterinformation planning . In addressing IO deconfliction, JP 3-13, *Joint Doctrine for Information Operations* states:

> IO deconfliction may be required at several levels, i.e., within, above, and below the joint force, and at several levels of war. In addition, offensive and defensive IO may need to be deconflicted at the same level. As with integration, deconfliction of IO should begin at the earliest possible stage of IO planning. (V-10)

JP 3-13 goes into further detail as to how deconfliction may be accomplished. The model however, does not address how IO deconfliction should be handled at any level of war or how it should be handled between offensive and defensive counterinformation objectives. Failure to deconflict IO plans and resources within the Air Force, and in the larger context of joint operations could be counterproductive to achieving information superiority and national security objectives.

2. The model is missing pre-crisis Air Force-level operations planning guidance. AFDD 2-5, *Information Operations* states that an Air Force IW team will be established during a crisis at the component level and that this team will integrate Air Force IW activities into a joint air and space operations plan. (25). It further states that this

team develops IW courses of action (COAs) based on Commander Air Force Forces (COMAFFOR)-assigned tasks to meet Joint Forces Commander (JFC) objectives (26).

It appears that the model assumes that all crises will involve Joint integration and rely on evolving Joint-level plans or Joint-level planning guidance such as the Joint Operation Planning and Execution System (JOPES) as the crisis unfolds. In the model there is no identification of, or reference to Air Force IO planning guidance to make this transition happen, nor to support crisis situations not involving joint operations.

3. The model does not address IO training or exercise support. JP 3-13 quotes Department of Defense Directive (DODD) S-3600.1, *Information Operations* in reference to training and exercises:

> Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure that commanders of US Armed Forces are well-informed about trade-offs among affecting, exploiting, and destroying adversary information systems, as well as the varying capabilities and vulnerabilities of DOD information systems. (VI-1)

JP 3-13 outlines specific guidance for joint IO training and exercises including offensive and defensive IO training, IO in joint exercises, and IO in planning and exercise modeling and simulation. It also reiterates Chairman of the Joint Chiefs of Staff-specific IO policy which states that Service school curricula will ensure personnel are educated in the concepts of IO in peace and IW during crisis and

conflict, and that Services will integrate IO into exercises to enhance overall joint operational readiness (I-7 and I-12).

The 1996 Air Force whitepaper entitled *Information Warfare* states that there are three goals to guide the Air Force in mastering IW, one of which includes building organizations with equipment, procedures and trained personnel prepared to plan and execute IW in support of the CINC's campaign objectives (15).

The report of the Defense Science Board Task Force on IW made several recommendations with training and exercise implications such as developing and implementing simulations to demonstrate the effects of defensive IW, and implementing policy to include defensive IW realism in exercises (3e and 3f).

AFDD 1, *Air Force Basic Doctrine* in discussing the definition of doctrine states that air and space doctrine shapes the manner in which the Air Force organizes, trains, equips, and sustains its forces (3).

As a member of the joint team, the Air Force will certainly be called upon to participate in joint IO training and exercises. As part of the Air Force's operational doctrine, AFDD 2-5 should specifically address in-service and joint-integrated IO training and exercise support.

4. The model does not provide guidance on Civil Affairs (CA), Public Affairs (PA), and news media interaction. These areas have been combined in this discussion because they are all related IO functional concerns within the IO environment.

JP 3-13 states that CA are important to IO because of their ability to interface with key organizations and individuals in the information environment and that CA can

support and assist IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas (I-32). JP 3-13 also states that coordination of PA and IO plans is required to ensure that PA initiatives support the commander's overall objectives (I-32). JP 3-13 further states that the news media can have significant impact on national will, political direction, and national security objectives and policy (I-32).

The Army refers to CA and PA as specific operations that contribute to gaining and maintaining information dominance in FM 100-6, *Information Operations* (3-0).

The Air Force model does not provide guidance on these elements of the information environment, or their historical relevance and future implications with regard to the principles of war and achievement of information superiority and national security objectives.

5. The model does not adequately address legal considerations. The Air Force model does not adequately address the legal implications of conducting offensive and defensive IO at various levels of conflict. It provides no guidance on how the Law of Armed Conflict (LOAC) may be applied across a range of IO capabilities at various levels of crisis and does not address integration with the range of law enforcement agencies that may be involved in IO activities, such as the Office of Special Investigations, Federal Bureau of Investigation, Central Intelligence Agency, and National Security Agency. Although it suggests a Judge Advocate General presence on an IW team that may form during crisis, no principles or planning guidance are given to suggest what this presence will do.

In discussing constraints FM 100-6, *Information Operations* states that statutory constraints, international law, federal regulations, and rules of engagement may limit a commander's options regarding IO (6-4). The author of *The International Legal Implications of Information Warfare* states that many legal issues raised regarding IW are without precedent, and that most of the law that legal scholars look to for guidance was developed long before IW concepts were envisioned (109).

The report of the Defense Science Board Task Force on IW recommended as part of defining threat conditions and responses that legislative and regulatory implications be explored (13). The forum for addressing IO legal responsibilities and considerations includes doctrine and policy, and as such doctrine and policy is incomplete without it..

6. How joint IO cell support will be accomplished is not clearly stated by the model. JP 3-13 states that Service component commanders should organize their staffs to plan and conduct IO, including the appointment of an IO point of contact or IO officer to interface with the joint IO cell (IV-12). The Air Force model does not state who the IO interface will be or how coordination with the joint IO cell will be accomplished.
7. The model does not explain reachback capability. As part of functions supporting IO, AFDD 2-5, *Information Operations* states that other agencies and organizations such as the NSA may provide support and/or reachback to the COMAFFOR IW team without ever expanding on what type of reachback capability could be provided, or how it could be accomplished (21). It also does not address the difference between reachback and support.

Consistent. For the model to be consistent it must apply the same definitions, terminology, and concepts as governing doctrine. Focus of the analysis regarding consistency was on AFDD 2-5, *Information Operations* as this document is still in draft form and as such inconsistencies can be addressed before it is published. Also, there is a two-year gap between the publishing of *Cornerstones of Information Warfare* and draft 4 of AFDD 2-5, in which, the evolution of terms and concepts has resulted in some change. In general, AFDD 2-5 was consistent with governing doctrine such as JP 3-13 and AFDD 1 in its use of the same definitions, terminology, and concepts. The following inconsistencies were identified during the congruence analysis:

1. Information. AFDD 2-5 defines information as

> 1. Unprocessed data of every description which may be used in the production of intelligence. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (40)

JP 3-13 defines information as

> 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (GL-11)

Although the second definitions above match, the first definitions are conceptually inconsistent. The AFDD 2-5 definition suggests that information is limited to unprocessed data and does not account for processed data as having meaning or value or being considered information. That information may be used for the production of intelligence is a specific example of use rather than a root part of a

definition. The JP 3-13 definition places no limitations on what information is or how it may be applied.

2. Information Operations versus Counterinformation operations. The use of the terms counterinformation, offensive counterinformation and defensive counterinformation is peculiar to the Air Force. AFDD 2-5 defines counterinformation as "offensive and defensive information operations/information warfare activities which are conducted to establish information control" (39). Offensive counterinformation (OCI) is defined as "offensive IO/IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems" (41). Defensive counterinformation (DCI) is defined as "activities which are conducted to protect friendly information and information systems" (39). At the Joint-level different terms are used to define the same concepts.

In JP 3-13, information operations (IO) are defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems" (GL-12). JP 3-13 defines offensive information operations as

> the integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. (GL-15)

JP 3-13 defines defensive information operations as

> a process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations include information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (GL-9)

The result is that the terms used to describe essentially the same concepts are inconsistent between the Air Force and Joint levels.

3. Information Assurance. AFDD 2-5 defines information assurance as

> those measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation (ability to confirm source of transmission and data). (40)

This same term is defined in JP 3-13 as

> information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (GL-11)

The AFDD 2-5 definition broadly defines Information Assurance as "measures" while the JP 3-13 is more specific, identifying Information Assurance as "information operations", and includes provision for restoration, protection, detection, and reaction capabilities.

4. IW team versus Joint IO cell. AFDD 2-5 describes an IW team as comprised of core, resident and non-resident members. This team supports the Joint Forces Commander's Joint IO cell. Both entities perform essentially the same function at their respective level; merging the expertise from a variety of staff elements including but not limited to Staff Judge Advocate, Public Affairs, Intelligence, Military Deception, Psychological Operations, Special Technical Operations, and Electronic Warfare (JP 3-13, IV-4, and AFDD 2-5, 26). The joint IO cell also has a slots for Service-level IO representatives (JP 3-13, IV-4).

Cohesive. There are internal and external aspects of cohesiveness. To be internally cohesive, principles, issues and concepts presented must be integrated within the model. External cohesiveness with respect to doctrine and policy refers to whether the concepts are presented such that significant relationships are addressed including links to parent or subordinate doctrine and policy and broader national security objectives. The focus of the analysis for cohesiveness was primarily on AFDD 2-5, *Information Operations*.

In general, the presentation of principles, issues and concepts in the model was not internally cohesive, lacking support in the form of doctrinal principles and lacking presentation of historical examples and lessons learned from the application of IW/IO concepts and capabilities. External cohesiveness was generally lacking in that few references to higher-level and lateral doctrine and policy were made regarding IW/IO concepts and capabilities to ensure seamless integration. No references were made to the

tactical doctrine the follows from the model. Specific areas where the model was found to not be cohesive are reported in the paragraphs that follow.

1. The Model has a vague statement of purpose. JP 3-13, *Joint Doctrine for Information Operations* states as part of its purpose, that it sets forth doctrine to govern the joint activities and performance of US armed forces, that it provides military guidance, and that it prescribes doctrine for joint operations and training (i). AFDD 1, *Air Force Basic Doctrine* states as part of its purpose, that it establishes general doctrinal guidance for the application of air and space forces in operations, and that it is the premier statement of US Air Force basic doctrine (2). It also states that operational doctrine is contained in the AFDD-2 series publications, which describe the organization of air and space forces and applies the principles of basic doctrine to military actions (4). AFDD 1 also states that operational doctrine guides the proper employment of air and space forces in the context of distinct objectives, force capabilities, broad functional areas, and operational environments, and that it provides focus for developing the missions and tasks that must be executed through tactical doctrine (4). Doctrine can be defined as fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives (JP 1-02). The preceding statements on purpose and the definition of doctrine provide a framework for identifying the purpose of AFDD 2-5, *Information Operations*, however the stated purpose of AFDD 2-5 is to explain the Air Force perspective on IO (v). This stated purpose is void of any links to associated doctrine in terms of context and does not identify the principles and guidance provided in it.

2. The model does not address interfacing doctrine. Although AFDD 2-5 references AFDD 2, *Global Engagement*, it does not address its relationship with it or AFDD 1, *Air Force Basic Doctrine*, both of which are direct parent doctrine. AFDD 2-5 also does not address its relationship with subordinate tactical doctrine. It references JP 3-13, as part of the joint guidance on IO but does not address how it interfaces with it. These relationships help establish a seamless presentation of principles and guidance within the doctrinal framework. When they are absent gaps can form and doctrine can become stove-piped, or developed in isolation.
3. The model does not relate IO to principles of war. Whereas AFDD 1 discusses the basic doctrinal implications of the principles of war, AFDD 2-5 does not address the IO doctrinal implications of the principles of war. Part of the purpose of doctrine is to provide historical precedence, warfighting principles, and accumulated knowledge (AFDD 1, 3). Although AFDD 2-5 does provide hypothetical examples of IO in warfare, such as giving an example of information attack as interjecting disinformation into a radar stream that causes antiaircraft missiles to miss intended targets, it does not provide examples related to the principles of war (11).
4. The model has a convoluted presentation of the nature of IO. AFDD 2-5 mentions information superiority as one of the Air Force's core competencies but does not relate it to the nature of IO or address how IO will help achieve information superiority (3). AFDD 2-5 also states that "the strategic perspective and the flexibility gained from operating in the air-space continuum make airmen uniquely suited for information operations," but does not support this statement or relate it to

the nature of IO (3). AFDD 2-5 states that the Air Force has embraced the concepts of IO and IW and then moves to referencing IO as offensive and defensive counterinformation without addressing the purpose in changing the terminology (1-3). AFDD 2-5 mentions the GII, NII, and DII, but does not mention the Air Force Information Infrastructure (AFII), nor does it discuss the interfaces between these infrastructures (2). AFDD 2-5 discusses IO threats but does not relate the threats to potential targets (4). IO targeting is only discussed as part of counterinformation planning (27-28). The information infrastructures and greater information environment, and IO threats are all fundamental to the nature of IO.

5. Principles of IO are not clearly outlined in the model. AFDD 2-5 discusses IO as offensive and defensive counterinformation without discussing the principles behind employing these measures. As previously mentioned, doctrine is founded in principles.
6. How national military objectives and information superiority will be accomplished through IO is not clearly stated in the model.

Summary of Analysis

By employing the Delphi technique, weaknesses in the intended object of analysis were addressed, and consensus was reached on a model for the criterion-based congruence analysis. This resulted in the use of the Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy as the object of analysis.

The criterion-based congruence analysis results suggest that the object of analysis is incongruent in several areas with the secondary source documents in terms of being complete, consistent and cohesive. The model is incomplete in the areas of deconfliction of responsibilities and application of resources in counterinformation planning, pre-crisis Air Force-level operations planning guidance, IO training and exercise support, guidance on Civil Affairs, Public Affairs and news media interaction, adequately addressing legal considerations, clearly stating how joint IO cell support will be accomplished, and explaining reachback capability.

The model lacks consistency in its definitions of information and information assurance, and in its use of the terms IW team and counterinformation.

The model is not cohesive in a number of areas. It appears that it has a vague statement of purpose, does not address interfacing doctrine, does not relate IO to principles of war, presents the nature of IO in a convoluted manner, does not clearly outline the principles of IO, and does not clearly state how information superiority and national military objectives will be accomplished through IO.

Chapter V discusses what was learned about the investigative questions, identifies the limitations of the study, and provides observations regarding Air Force IW doctrine and policy. It also suggests further research avenues.

V. Discussion

Discussion of the Investigative Questions

Based on the results of the criterion-based congruence analysis presented in Chapter IV, each of the four investigative questions is discussed below.

1. *Does Air Force IO and IW doctrine and policy flow naturally and consistently from guidance developed at higher levels?*

Congruence criteria for answering this question include *consistent* and *cohesive*. Directly above the Air Force level of doctrine and policy is the Joint level. Air Force doctrine and policy should be consistent with, and flow naturally from Joint doctrine and policy even though Air Force doctrine is largely developed from an aerospace paradigm.

There are several disconnects in the doctrine and policy model that was analyzed that detract from it flowing naturally and consistently with Joint doctrinal guidance such as JP 3-13, *Joint Doctrine for Information Operations*. These disconnects are discussed in the paragraphs below.

Chapter IV presented four examples of inconsistent use of terminology including different definitions of "information" and "information assurance" and the use of the terms "counterinformation" and "IW team" instead of "information operations" and "IO cell" to describe the same or similar concepts. The use of inconsistent definitions and terminology between the Joint and Service levels may confuse the warfighter and detract from joint operations.

The model lacks cohesiveness internally in that it seems to have a vague statement of purpose, does not clearly state the principles of IO, and has a convoluted presentation

of the nature of IO. It lacks external cohesiveness in that it does not address its relationship with interfacing doctrine such as AFDD 1, *Air Force Basic Doctrine*, AFDD 2, *Air and Space Power Organization and Employment,* or subordinate tactical doctrine, and only lists JP 3-13, *Joint Doctrine for Information Operations* as a reference

The model also does not clearly state how information superiority or national military objectives will be accomplished through IO. Thus, in terms of consistency and cohesiveness, there are several areas where the model does not appear to flow naturally and consistently from guidance developed at higher levels.

2. Is Air Force IO and IW doctrine and policy complete?

A single congruence criterion, *complete*, applies to this question. Chapter IV presented seven areas where the model was incomplete. Two of these areas concern planning; not addressing deconfliction of responsibilities and application of resources in information operations planning, and not addressing pre-crisis Air Force-level operations planning guidance.

The other incomplete areas include not addressing IO training and exercise support, not providing Civil Affairs, Public Affairs and news media interaction guidance, not adequately addressing legal considerations of IO, not clearly stating how Joint IO cell support will be accomplished, and not defining or explaining reachback capability or its significance to IO.

The absence of these areas in the model suggests that Air Force IO and IW doctrine and policy is incomplete.

3. Does Air Force IO and IW doctrine and policy address everyone it needs to at all appropriate levels?

A single congruence criterion, *complete*, is applicable to this question. As stated above, the model is incomplete in part because it does not address IO training and exercise support, Civil Affairs, Public Affairs, news media interaction guidance, legal considerations of IO, and Joint IO cell support. This suggests that Air Force IO and IW doctrine and policy does not address everyone it needs to at all appropriate levels.

4. Is Air Force IO and IW doctrine and policy consistent with our national strategic objectives and national security?

The congruence criteria that apply to this question are *cohesive* and *consistent*. As stated in Chapter IV addressing cohesiveness, how national military objectives and information superiority will be accomplished through IO is not clearly addressed in the model and its underlying documents.

Use of inconsistent definitions and terminology, such as the examples discussed in Chapter IV and in the answer to question 1 above, suggests there are fundamental differences in the way the Air Force and the Joint Staff view several IO concepts.

Whether these shortcomings translate directly into inconsistencies in addressing national strategic objectives and national security cannot be determined from the analysis that was conducted. However, by not clearly stating how national military objectives and information superiority will be achieved, and by using disparate terminology, the Air Force model leaves the question open for debate.

Observations

The goal of this research was to determine if unclassified current and pending Air Force IO and IW doctrine and policy is congruent with what has been mandated by military and political leaders and what has been reported about IO and IW in studies and commentary. It appears there are areas where Air Force IO and IW doctrine and policy can be improved in terms of being congruent.

Difficulties with both consistency and cohesiveness may be anchored in the underlying "air and space" paradigm the Air Force applies to doctrine and policy formation in favor of a "joint and national" approach. Part of the problem appears to be the use of terms and definitions that are inconsistent with those used in Joint doctrine. By aligning Air Force terminology with Joint and DOD terminology confusion can be avoided.

Unless a strong case can be made against it, use of the terms counterinformation, defensive counterinformation, and offensive counterinformation which are peculiar solely to the Air Force should be dropped in favor of information operations, defensive information operations and offensive information operations, or otherwise coordinated with Joint and DOD terms. The same argument applies to dropping "IW Team" and adopting the Joint term "IO Cell."

Air Force IO doctrine and policy should also address several IO planning issues in more detail, such as deconfliction of responsibilities and resources, pre-crisis planning, and exercise and training support. This would improve the completeness of the IO

doctrine and policy and clarify how the Air Force will support Joint information operations.

AFDD 2-5, *Information Operations* states that its purpose is to explain the Air Force perspective on IO. The purpose of military doctrine goes well beyond simple presentation of perspective; it is part history and part vision presented in the form of applied principles and theory and examples from past conflict presented in the form of lessons learned, and presents authoritative guidance for future application by warfighters. Air Force IO and IW doctrine and policy should present the history of information operations based on lessons learned, and offer authoritative guidance for warfighters that is clearly grounded in IO and IW principles.

Air Force IO and IW doctrine and policy should seamlessly integrate and clearly present how it supports national security and military objectives. *A National Security Strategy of Engagement and Enlargement*, the *National Military Strategy of the United States of America*, *Joint Vision 2010: America's Military Preparing for Tomorrow*, *Concept for Future Joint Operation: Expanding Joint Vision 2010,* and *Global Engagement: A Vision for the 21st Century Air Force* are a large part of the strategic planning framework available for plotting the course ahead.

Air Force IO and IW doctrine and policy should also specifically link the principles of war and the principles of IO to achieving and sustaining information superiority.

There are other influences to consider when developing IO/IW strategy, doctrine and policy such as information environments, technological advances, and global

economic and political climates, and history and vision. A more fundamental consideration is the role of Information Resource Management (IRM). These concepts can be combined into a framework based on a joint and national perspective. An example of this is presented in Figure 18. A Strategic Planning Framework for Doctrine and Policy Development.

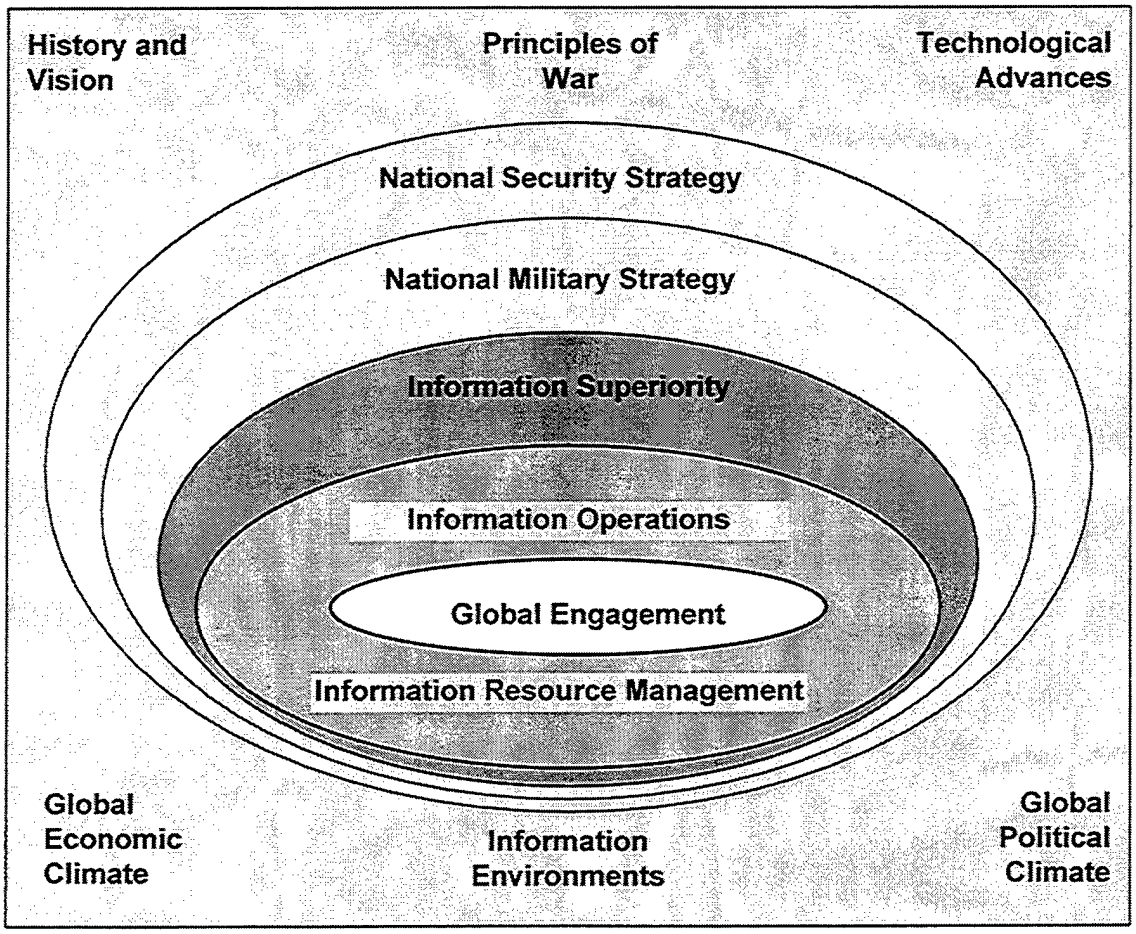


Figure 18. A Strategic Planning Framework for Doctrine and Policy Development

The strategic planning framework presented in Figure 18 begins with recognition of major factors that influence our National Security Strategy, National Military Strategy,

and current Air Force strategy of Global Engagement. Six of these factors are shown at the corners, and centered at the top and bottom of the figure. The National Security Strategy determines the National Military Strategy. Common to the services and agencies of the DOD is Information Superiority, part of the Joint concept of Full Spectrum Dominance. Global Engagement, the Air Force vision, flows from the National Security Strategy and is grounded in Joint Vision 2010 (Global Engagement, letter).

Information Superiority is also an Air Force core competency and critical component of Global Engagement. Critical to achieving and sustaining Information Superiority is the mastery of Information Operations. Recognizing that information is a critical resource, Information Resource Management is a means of efficiently and effectively planning, organizing, commanding, and controlling information and information technology, and directly supporting Information Operations. In sum, to achieve and sustain Information Superiority, an Information Operations Strategy grounded in IO doctrine and policy, and supported by fully integrated Information Resource Management, should be implemented.

Limitations of the Study

There are several limitations to this study that need to be addressed as they may impact its validity or applicability. These limitations are discussed in the paragraphs that follow.

First, no classified documents were reviewed or included in the congruence analysis. There are many classified works on the subjects of information warfare and

information operations that could influence a congruence analysis study's results. These documents include but are not limited to the following:

1. DODD S-3600.1, Information Operations
2. CJCSI 3210.01, Joint Information Warfare Policy
3. Appendix A to JP 3-13, Information Operations, draft 2

Second, the doctrine and policy development processes are inherently dynamic. Modeling with, making assessments with, and drawing conclusions from the draft output of such processes may impact the value or applicability of the results to the research problem. As one of the Delphi group members reported in the second round, multiple versions of AFDD 2-5, *Information Operations* (draft 4) are in circulation and several changes in the presentation of concepts were expected in subsequent draft releases.

Third, the methodology used in this study, criterion-based congruence analysis, although grounded in the work of Cooper and Emory, Miles and Huberman, and Dalkey, is essentially new and has no history of reliability. It was developed to fill a void in congruence-based qualitative data analysis methods for exploratory research. No assessment has been made on its usefulness.

The fourth limitation is also with regard to the methodology. Interpretation of, and application of, the congruence criteria are subjective processes, and as such, may yield some variation in findings among researchers.

Finally, there was potential for researcher bias to occur through field contacts prior to and during data collection, and through phone conversations with Delphi group members throughout the study in which general information warfare and information operations discussions took place.

Implications for Future Research

One of the limitations of this study was that it considered only unclassified materials in the data collection and analysis. Future research may include the addition of the full spectrum of classified documents. Also, several unclassified documents have been published since the closure of the data collection period, or were suggested for inclusion and were unable to be included. Some of these documents may be applicable to future research including:

1. Concept for Future Joint Operations: Expanding Joint Vision 2010, JCS, May 1997
2. Grand Strategy for Information Age National Security: Information Assurance for the Twenty-first Century. Lt Col Kevin J. Kennedy, Col Bruce M. Lawlor, USARNG; and Capt Arne J. Nelson, USN. AU Press Research Report, 1997.
3. Air Force Doctrine Document 1, Air Force Basic Doctrine, September 1997
4. Air Force Doctrine Document 2, Air and Space Power Organization and Employment, draft 7, 10 October 1997
5. CJCS MOP No. 30, Joint Command and Control Warfare, 8 Mar 1993 (canceled 30 Sep 96)
6. Information Operations Master Plan, ASD/C3I

Appendix A: Glossary of Terms and Acronyms

Unless otherwise noted, the source of all terms listed in this glossary is: The DOD Dictionary of Terms, http://www.dtic.mil/doctrine/jel/doddict/

doctrine: (DOD) Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)

global information infrastructure: (DOD) The worldwide sum of all interconnected information systems and the systems that connect them. Also called GII. See also information; information system. (Approved by JMTGM# 034-96)

information: Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in media. (CSAP CONOPS)

information assurance: Those measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation (ability to confirm source of transmission and data). (AFDD 2-5, draft 3)

information enhancement: Information Enhancement consists of operations and information systems that enhance force effectiveness such as: Intelligence, C^2, Precision Navigation and Positioning, Surveillance and Reconnaissance, and Weather. (AFDD 2-5, draft 3)

information operations: Those actions taken to affect adversary information and information systems while defending one's own information and information systems. (AFDD 2-5, draft 3)

information superiority: The ability to collect, control, exploit and defend information while denying an adversary the ability to do the same. (AFDD 2-5, draft 3)

information superiority: (DOD) That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (Approved by JMTGM# 034-96)

information systems: The means used to acquire, transform, store, or transmit information. (AFDD 2-5, draft 3)

information warfare: (DOD) Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and

computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW.
(Approved by JMTGM# 034-96)

information warfare: Action taken within the information environment to deny, exploit, corrupt, destroy, or assure information viability. (AFDD 2-5, draft 3)

malicious logic: Hardware, software, or firmware that is intentionally included or introduced into a system for unauthorized purposes. (CSAP CONOPS)

military deception: Those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or in-actions) that will contribute to the accomplishment of the friendly mission. (AFDD 2-5, draft 3)

military strategy: (DOD) The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force. See also strategy. (JP 1-02)

national military strategy: (DOD) The art and science of distributing and applying military power to attain national objectives in peace and war. See also military strategy; national security strategy; strategy; theater strategy. (JP 1-02)

national policy: (DOD) A broad course of action or statements of guidance adopted by the government at the national level in pursuit of national objectives. (JP 1-02)

national security strategy: (DOD) The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy. See also military strategy; national military strategy; strategy; theater strategy. (JP 1-02)

operations security: the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) Identify those actions that can be observed by adversary intelligence systems. b) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

psychological operations: Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (Joint Pub 1-02)

ACC: Air Combat Command

AETC: Air Education and Training Command

AFCERT: Air Force Computer Emergency Response Team

AFDC: Air Force Doctrine Center

AFII: Air Force Information Infrastructure

AFIT: Air Force Institute of Technology

AFIWC: Air Force Information Warfare Center

AFOSI: Air Force Office of Special Investigations

AIA: Air Intelligence Agency

ASIM: Automated Security Incident Measurement

ATO: Air Tasking Order

C2: command and control

C2W: command and control warfare

C4: Command, Control, Communications, and Computers

CERT: Computer Emergency Response Team

CIA: Central Intelligence Agency

CI: counterinformation

CJCS: Chairman of the Joint Chiefs of Staff

CMET: Countermeasures Engineering Team

CONOPS: Concept of Operations

CSAP: Computer Security Assistance Program

CSET: Computer Security Engineering Team

DCI: Defensive Counterinformation

DII: Defense Information Infrastructure

DOD: Department of Defense

ESST: Electronic Security Survey Team

FIRST: Forum for Incident Response Security Team

FIWC: Fleet Information Warfare Center

GII: Global Information Infrastructure, Geospatial Information Infrastructure

IA: Information Assurance

IADS: Integrated Air Defense System

IDT: Intrusion Detection Tools

IO: Information Operations

IP: Information Protection

IR: Incident Report

IW: Information Warfare

IWS: Information Warfare Squadron

JCS: Joint Chiefs of Staff

LIWA: Land Information Warfare Activity

LOAC: Law of Armed Conflict

MAJCOM: Major Command

MII: Military Information Infrastructure

NSA: National Security Agency

NIST: National Institute of Standards and Technology

NIWA: Naval Information Warfare Activity

NRO: National Reconnaissance Office

OCI: Offensive Counterinformation

OMB: Office of Management and Budget

Appendix B: Round 1 Delphi electronic mail cover letter

Dear (individual's name),

1. I am a graduate student at the Air Force Institute of Technology conducting research for the Air Force on current and pending Air Force information warfare doctrine and policy. Part of this research involves assessing the accuracy of a model of current and pending Air Force information warfare doctrine and policy, and checking the completeness of a secondary source listing. I would greatly appreciate your assistance in conducted this part of my research. No comments will be attributed to you or your organization.

2. The attached file named Model.doc is a Microsoft Word 6.0 document. It contains a model of current and pending Air Force information warfare doctrine and policy and a brief description of the model. Below the description are two questions regarding the model that I need your response to.

3. The attached file named List.doc is a Microsoft Word 6.0 document. It contains a list of secondary source documents I am using in my analysis. At the end of the list there is a question regarding its completeness. Your response to this question is also necessary for my research.

4. If possible, please return your comments by October 28th. The attached documents do not need to be returned unless you find it useful to do so in your response. A simple e-mail response may also be used. I will then consolidate the comments and incorporate them into the model. If there are significant improvements, I will send the improved model out for your assessment. The List.doc will not be resent.

5. I may be reached at 937-236-4657, or kpeifer@afit.af.mil. My thesis advisor and program manager for Information Resource Management is Dr. Alan Heminger, who may be reached at 937-255-1210, or aheminge@afit.af.mil.

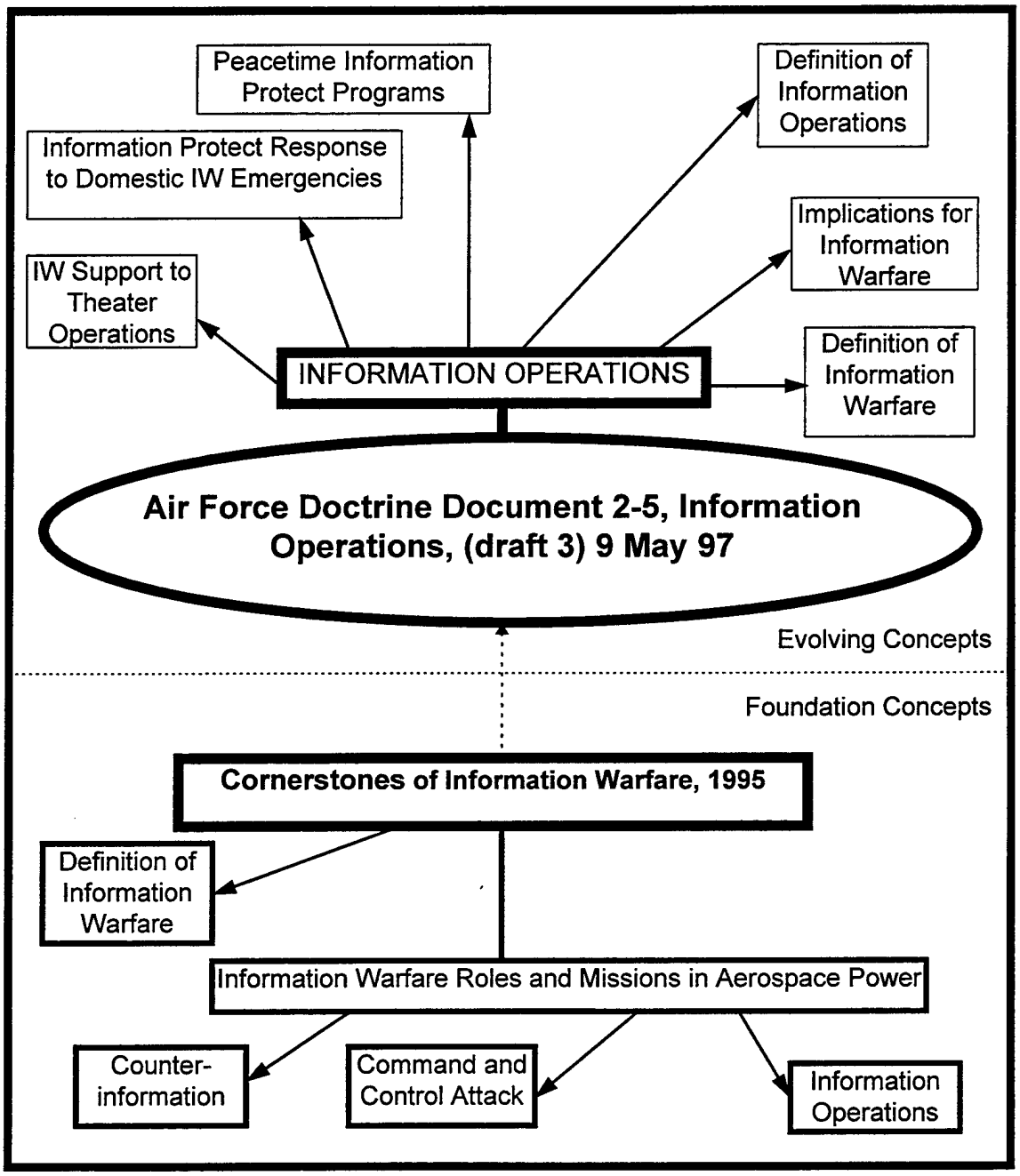
6. At your request, a completed copy of my thesis will be sent to you by electronic mail (zipped as Microsoft Word 6.0). Please indicate if you are interested in your response. I am scheduled to graduate on December 16th, and hope that I will be sending my final thesis during the beginning half of December.

Again, thank you very much for your assistance.

KENNETH V. PEIFER, Captain, USAF
Graduate Student, Air Force Institute of Technology

Appendix C: Original Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy

Document Name: Model.doc



DESCRIPTION: This model was developed by examining 46 unclassified documents that discuss Air Force information warfare doctrine, policy, concepts and strategy, and then selecting those that best exemplified doctrine and policy by content and description. This resulted in the selection of two documents:

1. *Cornerstones of Information Warfare,* an Air Force white paper, was developed in 1995, and is the Air Force's first unclassified document that directly addressed doctrine and policy issues. At the unclassified level, it represents the origin of IW doctrine and policy of the Air Force. The model depicts this document as a foundation.

2. AFDD 2-5, *Information Operations*, represents current thinking with regard to IW doctrine and policy. IW has become a subset of Information Operations. The model depicts this document as grounded in, but a clear departure from *Cornerstones of Information Warfare*. Still in draft form, its release is pending final approval.

Question 1: In your professional opinion, does this model capture the core unclassified documents of current and pending Air Force information warfare doctrine and policy? Yes or No.

Question 2: (Only need to answer if your answer to Question 1 is No) Which specific unclassified documents are necessary to complete the model?

Appendix D: A Suggested Chronology of Key IO/IW Doctrine and Policy Guidance

Document Name: List.doc

#	Date	Title
1	Mar 92	Basic Aerospace Doctrine of the United States Air Force, AFM 1-1
2	12 Aug 93	Air Force Policy Directive 10-7, *Operations*, Command and Control Warfare
3	95	Information Warfare, Airpower Journal, George J. Stein
4	95	Joint Vision 2010, America's Military Preparing for Tomorrow (JCS JV 2010)
5	95	New World Vistas, Air and Space Power for the 21st Century, Information Applications Volume
6	95	New World Vistas, Air and Space Power for the 21st Century, Information Technology Volume
7	95	National Military Strategy of the United States (JCS)
8	95	USAF Fact Sheet 95-20, Information Warfare
9	10 Jan 95	Joint Publication 1, Joint Warfare of the Armed Forces of the United States
10	1 May 95	Information Warfare: An Opportunity for Modern Warfare, ACSC/DEC/020/95-05
11	30 May 95	Joint Publication 6, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations
12	Jun 95	Cornerstones of Information Warfare
13	1 Oct 95	Air Force Policy Directive 14-1, Intelligence, Air Force Intelligence Planning and Operations
14	96	The International Legal Implications of Information Warfare
15	96	Information Warfare: The Next Major Change in Military Strategies and Operational Planning
16	96	Strategic Information Warfare: A New Face of War
17	96	Information War and the Air Force: Wave of the Future? Current Fad?, RANDIP-149
18	96	The Advent of Netwar, RAND MR-789-OSD
19	96	Security in Cyberspace: Challenges for Society, Proceedings of an International Conference
20	96	Information Warfare (USAF)
21	96	Information Warfare, A Strategy for Peace, The Decisive Edge in War
22	Feb 96	A National Security Strategy of Engagement and Enlargement
23	7 Feb 96	Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare C2W
24	8 Feb 96	Office of Management and Budget Circular No. A-130
25	1 Apr 96	Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach

26	1 Apr 96	The Need For a USAF Information Warfare (IW) Strategy For Military Operations Other Than War MOOTW
27	1 Apr 96	Information Warfare in a Joint and National Context
28	15 Apr 96	Information Warfare and the Lack of a U.S. National Policy
29	May 96	Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84
30	1 May 96	Air Force Doctrine Document 50, Intelligence
31	31 May 96	Chairman of the Joint Chiefs of Staff Instruction 6510.01A, Defensive Information Warfare Implementation
32	Jun 96	Assessments Necessary in Coming To Terms with Information Warfare
33	4 Jul 96	Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Ed. SAIC No. MDA903-93-D-0019
34	15 Jul 96	Executive Order 13010, Critical Infrastructure Protection
35	27 Aug 96	Field Manual No. 100-6 Information Operations
36	Oct 96	From Hackers to Projectors of Power, Information Warfare
37	Nov 96	Global Engagement: A Vision for the 21st Century Air Force (AFCS)
38	25 Nov 96	Report of the Defense Science Board Task Force on Information Warfare
39	1 Dec 96	Air Force Policy Directive 33-2, Information Protection
40	97	Air Force Long Range Plan 1997
41	Apr 97	Computer Security Assistance Program Concept of Operations, CSAP CONOPS (draft v4), AFIWC/EA
42	May 97	A National Strategy for a New Century (NSC)
43	9 May 97	Air Force Doctrine Document 2-5, Information Operations (draft 3)
44	Jun 97	Joint publication 3-13, Joint Doctrine for Information Warfare, (draft 2)
45	24 Jun 97	AFDD 1 Basic Air Force Doctrine (final draft)
46	15 Jul 97	Joint Doctrine Capstone & Keystone Primer (CJCS)

After reviewing the above list of documents, please answer the following question. Question: Are there any unclassified documents that you believe are missing from the above list, that should be included in analyzing current and pending Air Force information warfare doctrine and policy? Yes/No

If you answered yes, please give the following information for each document if possible: Authors, title, publish date, a copy of the document, or identify where the document can be obtained, and a statement regarding its significance.

Appendix E: Round 2 Delphi electronic mail cover letter

Dear (individual's name),

Thank you for your input on the research I am conducting regarding analysis of unclassified current and pending Air Force information warfare doctrine and policy. As a result of the comments I have received I have attempted to improve the model of unclassified current and pending Air Force information warfare doctrine and policy.

I am attempting to build an accurate overview model of unclassified current and pending Air Force information warfare doctrine and policy. The model will be used as the object of analysis in my research. It will be compared with the documents on the list I sent to you last week.

The goal of the research is to obtain a qualitative measure of congruence in terms of completeness, consistency, and cohesiveness. I hope that this qualitative measure will indicate if the Air Force is moving in the right direction in terms of information warfare and information operations doctrine and policy development.

The attached file named I-Model.doc is a Microsoft Word 6.0 document. It contains the improved model of unclassified current and pending Air Force information warfare doctrine and policy and a brief description of the model. Below the description are two questions regarding the model that I need your response to.

If possible, please return your comments by November 7th. The attached document does not need to be returned unless you find it useful to do so in your response. A simple e-mail response may also be used. I will then consolidate the comments and incorporate them into the model. If there are significant improvements, I will send the improved model out again for your assessment.

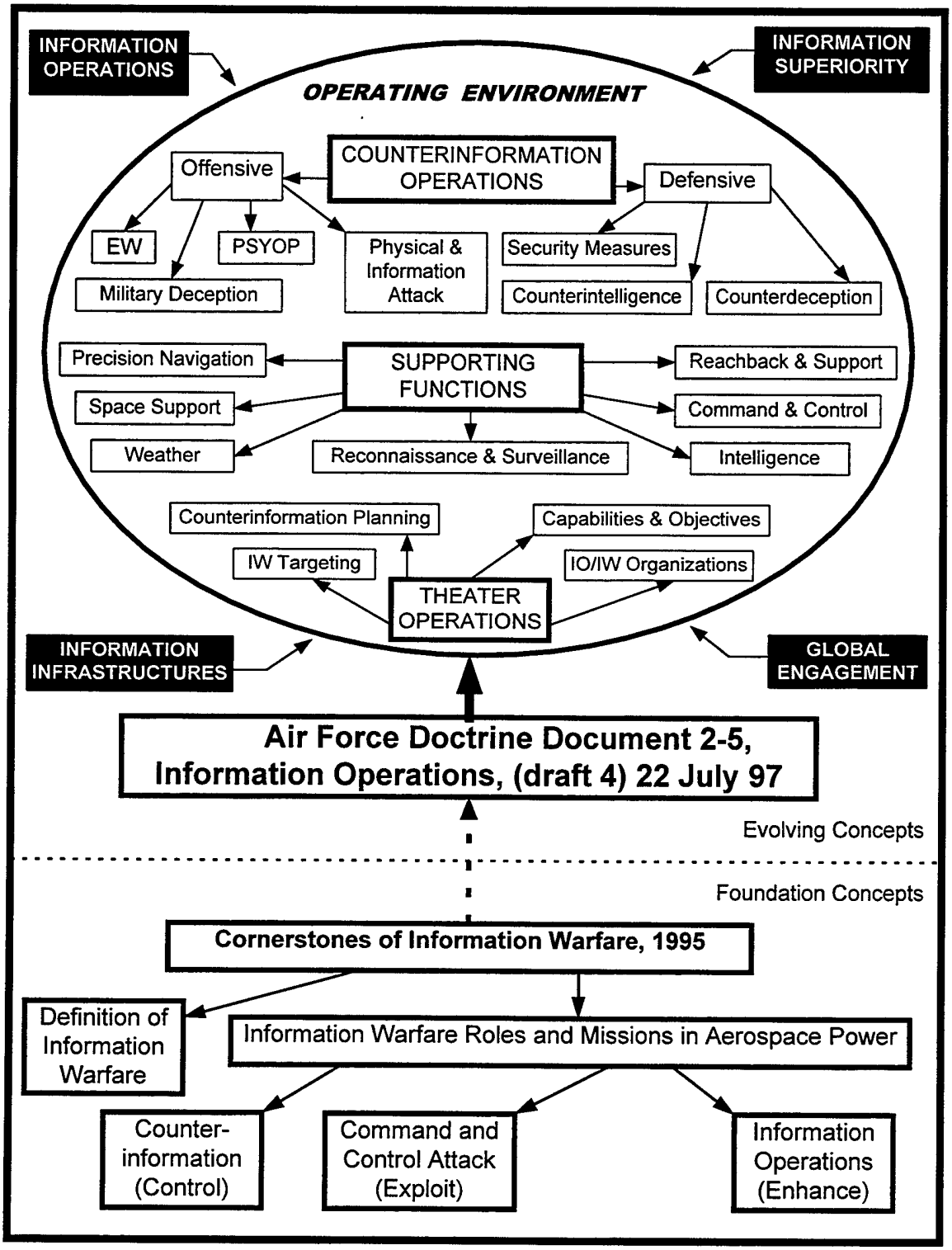
I may be reached at 937-236-4657, or kpeifer@afit.af.mil. My thesis advisor and program manager for Information Resource Management is Dr. Alan Heminger, who may be reached at 937-255-1210, or aheminge@afit.af.mil.

Again, thank you very much for your assistance.

KENNETH V. PEIFER, Captain, USAF
Graduate Student, Air Force Institute of Technology

Appendix F: Delphi-refined Model of Unclassified Current and Pending Air Force IO/IW Doctrine and Policy

Document Name: I-Model.doc



DESCRIPTION: This overview model was developed by examining 47 unclassified documents that discuss information warfare and information operations doctrine, policy, concepts and strategy, and then selecting those that best exemplified doctrine and policy by content and description. This resulted in the selection of two documents:

1. *Cornerstones of Information Warfare,* an Air Force white paper, was developed in 1995, and is the Air Force's first unclassified document that directly addressed doctrine and policy issues. At the unclassified level, it represents the origin of IW doctrine and policy of the Air Force. The model depicts this document as a foundation.

2. AFDD 2-5, *Information Operations*, represents current thinking with regard to IW doctrine and policy. IW has become a subset of Information Operations. The model depicts this document as grounded in, but a clear departure from *Cornerstones of Information Warfare*. Still in draft form, its release is pending final approval.

Question 1: In your professional opinion, does this model capture the *core unclassified documents* of current and pending Air Force information warfare and information operations doctrine and policy? Yes or No.

Question 2: (Only need to answer if your answer to Question 1 is No) Which specific unclassified documents are necessary to complete the model?

Bibliography

1. Aldrich, Richard W. (Maj, USAF). "The International Legal Implications of Information Warfare". Airpower Journal, 10:99-110 Fall '96.

2. Alger, John I. From Hackers to Projectors of Power. Information Warfare. Bulletin for the American Society for Information Science 23:5 Oct-Nov '96.

3. Arquilla, John and David Ronfelt. The Advent of Netwar. Santa Monica CA. Rand Corp, 1996. (Report MR-789-OSD).

4. Boldrick, Michael, R. (Col, USAF, Ret.). Information Warfare: The Next Major Change in Military Strategies and Operational Planning. Soldier-Scholar 3:11-19 Fall '96.

5. Buchan, Glenn. Information War and the Air Force: Wave of the Future? Current Fad? Santa Monica CA. Rand Corp, 1996. (Issue Paper Rand-IP-149).

6. Butler, Bradley L. (Col, USAF). The Need for a USAF Information Warfare Strategy for Military Operations Other Than War (MOOTW). Maxwell AFB AL. Apr 1996, (Air University (US) Air War College. Research Report).

7. Campen, Alan D. (Col, USAF, Ret.). Assessments Necessary in Coming to Terms With Information War: Strategy, Doctrine for Information Warfare Require Agreed Upon Definitions, Understanding. Signal 50:47-49 Jun '96.

8. Christian, Shelley (Maj), and others. Information Warfare: An Opportunity For Modern Warfare. ACSC Research Paper, ACSC/DEC/020/95-05, Air Command and Staff College, Maxwell AFB AL. 1 May 1995.

9. Cooper, Donald R. and William C. Emory. Business Research Methods. 5th ed. Chicago. Irwin, 1995.

10. Dalkey, Norman C. Delphi. The RAND Corporation, Santa Monica CA. October, 1967.

11. Davis, Harry J. (LCDR, USN). Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach. Maxwell AFB AL. April 1996. (Air University (US) Air War College. Research Report).

12. Department of the Air Force. Basic Aerospace Doctrine of the United States Air Force. AFM 1-1 Vol. I, Washington. March 1992.

13. Department of the Air Force. Information Warfare. HQAF/XOXD. (Air Force Doctrine Division) A Primer on Information Warfare. Washington. 1996.

14. Department of the Air Force. Air Force Basic Doctrine. 24 June 1997. (AFDD 1, Final draft).

15. Department of the Air Force. Operations: Command and Control Warfare. 12 August 1993. (AFDD 10-7).

16. Department of the Air Force. Air Force Fact Sheet 95-20: Information Warfare. http://www.af.mil:80/news/factsheets/Information_Warfare.html, 10 September 1997.

17. Department of the Air Force. Information Protection. 1 December 1996. (AFPD 33-2).

18. Department of the Air Force. The 1997 Air Force Long-Range Plan: Summary. http://www.xp.hq.af.mil/xpx/7frame.htm, 13 October 1997.

19. Department of the Air Force. Air Intelligence Agency/Air Force Information Warfare Center. Computer Security Assistance Program (CSAP) Concept of Operations (CONOPS. Draft version IV, April 1997.

20. Department of the Air Force. Secretary of the Air Force/Air Force Chief of Staff. Global Engagement: A Vision For The 21st Century Air Force. http://www.xp.hq.af.mil/xpx/21/nuvis.htm, 13 October 1997.

21. Department of the Air Force. Information Operations. 9 May 1997. (AFDD 2-5, third draft).

22. Department of the Air Force. Information Operations. 22 July 1997. (AFDD 2-5, fourth draft).

23. Department of the Air Force. Cornerstones of Information Warfare. Washington, 1995.

24. Department of the Air Force. Intelligence. Washington. Government Printing Office. 1 May 1996. (AFDD 50)

25. Department of the Air Force. Air Force Information Warfare Center. 1997 Mission and Goals. http://www.aia.af.mil/aiaweb/homepages/afiwc/iwc_msn.htm. 20 June 1997.

26. Department of the Air Force. Air Force Information Warfare Center. Overview briefing of AFIWC presented to Capt. Peifer by 1Lt. Tidwell at AFIWC, Kelly AFB, San Antonio TX. 7 Aug 97.

27. Department of the Air Force. Air Force Information Warfare Center. Vulnerabilities and Solutions: 1996 AFIWC Information Protection Operations Summary. http://kumi.kelly.af.mil/lessons.html. 20 June 1997.

28. Department of the Air Force. Intelligence: Air Force Intelligence Planning and Operations. Washington. Government Printing Office. 1 Oct 1995. (AFPD 14-1).

29. Department of the Air Force. Linhard, Robert., Maj Gen, USAF, Director of Plans, (XOX), Deputy Chief of Staff for Plans & Operations. Doctrine Update. Briefing slides, 30 April 1996. Air University, Maxwell AFB AL. http://www.cdsar.af.mil/presentation/linhart/, 14 Sep 1996.

30. Department of the Air Force. New World Vistas: Air and Space Power for the 21st Century: Information Applications Volume. Washington. 1995.

31. Department of the Air Force. New World Vistas: Air and Space Power for the 21st Century: Information Technology Volume. Washington. 1995.

32. Department of the Army. Information Operations. FM 100-6, Washington. 27 August 1996.

33. Executive Order 13010. Critical Infrastructure Protection. Washington: Government Printing Office. 15 July 1996.

34. Federal Information Exchange. New World Vistas Study. http://web.fie.com/htdoc/fed/afr/sab/edu/text/any/afrtnwv.htm, 20 June 1997.

35. General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington. May 1996. (AIMD-96-84)

36. Hundley, Richard and others. Security in Cyberspace: Challenges for Society: Proceedings of an International Conference. Santa Monica CA. Rand Corp, 1996. (Report CF-128-RC).

37. Libicki, Martin C. What Is Information Warfare? Washington, Institute for National Strategic Studies, National Defense University. Washington. August, 1995. http://www.ndu.edu/ndu/inss/insshp.html, 20 June 1997.

38. Merriam-Webster Inc. WWWebster Dictionary - Search screen. Search results for congruence. Http://www.m-w.com/cgi-bin/dictionary. 17 October 1997.

39. Miles, Matthew B. and Micheal A Huberman. Qualitative Data Analysis: An Expanded Sourcebook. 2nd ed. Thousand Oaks CA. SAGE, 1994.

40. Molander, Roger C. et al. Strategic Information Warfare: A New Face of War. Parameters, Autumn 1996, pp.81-92.

41. Office of Management and the Budget. Management of Federal Information Resources. OMB Circular No. A-130. Washington: Government Printing Office. 8 February 1996.

42. President of the United States. A National Security Strategy of Engagement and Enlargement. Washington. February 1996.

43. President of the United States. A National Strategy for a New Century. Washington. May 1997.

44. Schwartau, Winn. Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. 2d ed. New York. Thunder's Mouth Press, 1996.

45. Science Applications International Corporation (SAIC). Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. 2d ed. Washington. 4 July 1996.

46. Stein, George J. "Information Warfare". Airpower Journal, Spring 1995, pp. 30-39.

47. Stoll, Clifford. The Cuckoo's Egg; Tracking a Spy Through the Maze of Computer Espionage. New York. Doubleday. 1989.

48. Tzu, Sun (Griffith, Samuel B., trans.) The Art of War New York: Oxford University Press. 1963.

49. United States. Defense Science Board. Report of the Defense Science Board Task Force On Information Warfare – Defense (IW-D). Washington, Office of the Under Secretary of Defense for Acquisition & Technology, Nov 1996. http://jya.com/iwd.htm. 20 June 1997.

50. United States. Chairman of the Joint Chiefs of Staff. Information Warfare: A Strategy for Peace, the Decisive Edge in War. JCS Brochure. Washington. 1996.

51. United States. Chairman of the Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington. 1995.

52. United States. Chairman of the Joint Chiefs of Staff. Joint Vision 2010: America's Military Preparing for Tomorrow. Washington. 1995.

53. United States. Joint Chiefs of Staff. Joint Doctrine Process. Joint Chiefs of Staff World Wide Web page, Joint Doctrine Process hyperlink. http://www.dtic.mil/doctrine/docinfo/process/procchart.htm. 16 Aug 1997.

54. United States. Joint Chiefs of Staff. Joint Doctrine Hierarchy. http://www.dtic.mil/doctrine/docinfo/pstatus/hierchart.htm. 16 Aug 1997.

55. United States. Joint Chiefs of Staff. Joint Doctrine Capstone & Keystone Primer. http://www.dtic.mil/doctrine/jel/c_pubs.htm. 13 October 1997.

56. United States. Joint Chiefs of Staff. Joint Warfare of the Armed Forces of the United States. Washington. 10 January 1995. (JCS Pub 1).

57. United States. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Washington. 30 May 1995. (JCS Pub 6).

58. United States. Joint Chiefs of Staff. Joint Doctrine of Information Operations. Washington. June 1997. (JP 3-13. Second draft).

59. United States. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). Washington. 7 February 1996. (JP 3-13.1).

60. United States. Joint Chiefs of Staff. Defensive Information Warfare Implementation. Washington. 31 May 1996. 1 vol. (CJCSI 6510.01a).

61. WarRoom Research, LLC. 1996 Information Systems Security Survey Conducted by WarRoom Research LLC in Cooperation with the U.S. Senate's Permanent Subcommittee on Investigations. http://www.warroomresearch.com/WRR/SurveysStudies/1996ISS_Survey_Summary Results.htm. 20 June 1997.

62. Wells, Daniel W. (Col, USA). Information Warfare in a Joint and National Context. Maxwell AFB AL. 1 Apr 1996. (Air University (US) Air War College. Research report).

63. Whisenhunt, Robert H. (Lt Col, USA). Information Warfare and the Lack of a U.S. National Policy. Carlisle Barracks PA. 15 Apr 1996. (U.S. Army War College. Strategy research project).

Vita

Captain Kenneth V. Peifer was born 27 August 1963 in New Britain, Connecticut. He graduated from St. Paul Catholic High School in Bristol, Connecticut in May 1981. He graduated Magna Cum Laude earning a Bachelor of Science degree in Management Information Systems from Central Connecticut State University in May 1992. He was a Distinguished Graduate from the Air Force Reserve Officer Training Corps program at the University of Connecticut and earned a Regular commission in May 1992.

As a Second Lieutenant, he graduated from Undergraduate Space Training at Lowry Air Force Base, Colorado in April 1993. He was assigned as a Missile Warning Operations Crew Commander at the 6th Space Warning Squadron, Cape Cod Air Station in May 1993, and became Chief of Standardization and Evaluation for Missile Warning Operations in 1995.

He entered the Information Resources Management program at the Graduate School of Logistics and Acquisition Management at the Air Force Institute of Technology in May 1996.

Permanent Address: 60 La Cava Road
Bristol, CT 06010

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1997	Master's Thesis

4. TITLE AND SUBTITLE
AN ANALYSIS OF UNCLASSIFED CURRENT AND PENDING AIR FORCE INFORMATION WARFARE AND INFORMATION OPERATIONS DOCTRINE AND POLICY

5. FUNDING NUMBERS

6. AUTHOR(S)
Captain Kenneth V. Peifer

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
2750 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GIR/LAS/97D-10

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFIWC/EA
Kelly AFB TX 78241

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 Words*)

This study focused on determining if unclassified current and pending Air Force information warfare and information operations doctrine and policy is moving in the direction it should in terms of being complete, consistent and cohesive based on what has been mandated and studied about information warfare. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was examined through criterion-based congruence analysis to make this determination. Investigative questions were developed in reference to the current state of unclassified Air Force information warfare and information operations doctrine and policy. Secondary data analysis was conducted along two paths. The hierarchical path included an examination of unclassified information warfare and information operations doctrine, policy and regulatory guidance. The academic path included an examination of studies and commentary on information warfare and information operations focusing on doctrine and policy. A model of unclassified current and pending Air Force information warfare and information operations doctrine and policy was developed. Then the model was analyzed for congruence in terms of completeness, consistency, and cohesiveness using the hierarchical and academic secondary data analysis as a diagnostic tool. The model was found to be partially incongruent in all three areas.

14. SUBJECT TERMS
Information, Warfare, Military Doctrine, Military Intelligence, Electronic Warfare, Delphi Technique

15. NUMBER OF PAGES
177

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

AFIT Control Number AFIT/GIR/LAS/97D-10

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?
a. Yes b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years_____ $_____

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

_____ _____
Name and Grade Organization

_____ _____
Position or Title Address